Middle-East Journal of Scientific Research 23 (8): 1741-1748, 2015
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2015.23.08.22470

Black Hole Attack Performance Evaluation and Degradation in Wireless Sensor Networks

[1]S. Rajanarayanan and [2]C. Suresh Gnana Dhas

[1]Department of Computer Science and Engineering, St.Peters University, Chennai, India
[2]Department of Computer Science and Engineering, Vivekandha college of Engineering, India

Abstract: Wireless sensor networks (WSN) is fast developing vicinity of research due to the tremendous number of applications that can greatly benefit from such systems and has lead to the development of tiny, cheap, disposable and self-contained battery powered sensor nodes. One of the major challenges WSNs face today is security. The problem of security is due to the wireless nature of the sensor networks and the inherent power and memory limitations of sensor nodes makes conventional security solutions unfeasible. Thus, the network is susceptible to attacks by malicious nodes and packets are dropped in attacks like black hole attack. In this paper, it is proposed to evaluate the performance of a network under the impact of malicious nodes.

Key words: Wireless Sensor Network (WSN) · Attacks · Black hole attack · Performance

INTRODUCTION

A Wireless Sensor Network (WSN) may comprise thousands of sensor nodes. Each sensor node has a sensing capability as well as limited energy supply, compute power, memory and communication ability. Besides military applications, WSN may be used to monitor microclimates and wildlife habitats, the structural integrity of bridges and buildings, building security, location of valuable assets (via sensors placed on these valuable assets), traffic and so on. However, realizing the full potential of WSNs poses myriad research challenges ranging from hardware and architectural issues, to programming languages and operating systems for sensor networks, to security concerns, to algorithms for sensor network deployment, operation and management [1].

The WSN do share some commonalities with general ad hoc networks. Thus, protocol design for sensor networks must account for the properties of ad hoc networks, including the following.

- Lifetime constraints imposed by the limited energy supplies of the nodes in the network.
- Unreliable communication due to the wireless medium.

Need for self-configuration, requiring little or no human intervention.

Incorporating these unique features of sensor networks into protocol design is important in order to eficiently utilize the limited resources of the network.

At the same time, to keep the protocols as light-weight as possible, many designs focus on particular subsets of these criteria for different types of applications. This has led to quite a number of different protocols from the data-link layer up to the transport layer, each with the goal of allowing the network to operate autonomously for as long as possible while maintaining data channels and network processing to provide the application's required quality of service [2].

WSN fall in three major categories called periodic sensing, query sensing and event sensing. In periodic sensing monitoring is always done by the sensor which monitors physical environment and continuously reporting measurement to the sink. In event sensing sensor operate in an silent monitoring state and are programmed to notify about event, such as the presence of the object in intrusion detection. In query based sensor reacts to the queries of the sink by returning the corresponding measurement. When an event is occur in the sensor field source node generated data and make the announcement to the sink that subscribing the data and

Corresponding Author: S. Rajanarayanan, Department of Computer Science and Engineering, St.Peters University, Chennai, India.

this whole process is known as data dissemination. Many data dissemination techniques have been proposed for sensor networks to explore in-network query processing, distributed data storage and approximation techniques [3-5].

Traditional (or flat) routing protocols for WSN may not be optimal in terms of energy consumption. Clustering can be used as an energy-efficient communication protocol [6]. The objectives of clustering are to minimize the total transmission power aggregated over the nodes in the selected path and to balance the load among the nodes for prolonging the network lifetime. Clustering is a sample of layered protocols in which a network is composed of several clumps (or clusters) of sensors. Each cluster is managed by a special node or leader, called cluster head (CH), which is responsible for coordinating the data transmission activities of all sensors in its clump. All sensors in a cluster communicate with a cluster head that acts as a local coordinator or sink for performing intra-transmission arrangement and data aggregation. Cluster heads in tern transmits the sensed data to the global sink. The transmission distance over which the sensors send their data to their cluster head is smaller compared to their respective distances to the global sink. Since a network is characterized by its limited wireless channel bandwidth, it would be beneficial if the amount of data transmitted to the sink can be reduced. To achieve this goal, a local collaboration between the sensors in a cluster is required in order to reduce bandwidth demands [7].

A hierarchical approach breaks the network into clustered layers [8]. Nodes are grouped into clusters with a cluster head that has the responsibility of routing from the cluster to the other cluster heads or base stations. Data travel from a lower clustered layer to a higher one. Although, it hops from one node to another, but as it hops from one layer to another it covers larger distances. This moves the data faster to the base station. Theoretically, the latency in such a model is much less than in the multihop model. Clustering provides inherent optimization capabilities at the cluster heads. In the cluster-based hierarchical model, data is first aggregated in the cluster then sent to a higher-level cluster-head. As it moves from a lower level to a higher one, it travels greater distances, thus reducing the travel time and latency. This model is better than the one hop or multi-hop model.

A cluster-based hierarchy moves the data faster to the base station thus reducing latency than in the multi-hop model. Further, in cluster-based model only cluster-heads performs data aggregation whereas in the multi-hop model every intermediate node performs data aggregation. As a result, the cluster-based model is more suitable for time-critical applications than the multi-hop model. However, it has one drawback, namely, as the distance between clustering level increases, the energy spent is proportional to the square of the distance. This increases energy expenditure. Despite this drawback, the benefits of this model far outweigh its drawback. A cluster-based hierarchical model offers a better approach to routing for WSNs.

In a typical sensor network application, sensors are to be placed (or deployed) so as to monitor a region or a set of points. It is desirable that the deployed collection of sensors be able to communicate with one another, either directly or indirectly via multi hop communication [9]. WSN are vulnerable to security attacks due to the broadcast nature of the transmission medium. Basically attacks are classified as active attacks and passive attacks. The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature. The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack [10].

Many sensor network routing protocols are quite simple and for this reason are sometimes even more susceptible to attacks against general ad-hoc routing protocols. Most network layer attacks against sensor networks fall into one of the following categories [11]:

- Spoofed, altered, or replayed routing information
- Selective forwarding
- Sinkhole attacks
- Sybil attacks
- Wormholes
- HELLO flood attacks
- Acknowledgement spoofing

Common network attacks include blackhole, grey hole and wormhole attacks and IP spoofing. Blackhole attacks are those when malicious nodes refuse to forward traffic [12]. External attacks can be prevented by using security mechanisms like firewalls and encryption. Internal attacks are more severe as malicious insider nodes of the network which are authorized and hence protected by the network's security services. Such malicious insiders who can operate in groups may use security means to protect their attacks. Such malicious parties are called compromised nodes, as their actions compromise network security.

In black hole attacks, a malicious node uses routing protocols to advertise itself as having the shortest path to a destination node or to a packet it wants to intercept. Such hostile nodes advertise availability of fresh routes without checking the routing table. Thus an attacker node always has the availability to reply to the route request thereby intercepting and retaining the data packet. In flooding, a malicious node's reply will be received by the requesting node before receipt of reply from the real node leading to a malicious and forged route creation. When this route is established it is now upto the node to ensure whether to drop all packets or forward it to the unknown address [13].

In this paper, it is proposed to evaluate the performance of a WSN under the impact of black hole attack. Simulations are conducted to evaluate the performance degradation of WSN due to malicious node activity. Section 1 dealt with the basics of the WSN and attacks in WSN, section 2 reviews some related works available in the literature. Section 3 details the methods used for evaluation, section 4 gives the simulation result and discusses the same. Section 5 concludes the paper.

Related Works

Survey on Black Hole Attack Detection in WSN: In hello flood attack, an adversary, which was not a legal node in the network, can flood hello request to any legitimate node and break the security of WSN. The current solutions for these types of attacks are mainly cryptographic, which suffer from heavy computational complexity. Hence they were less suitable for wireless sensor networks. Singh *et al*, [14] proposed a method based on signal strength has been proposed to detect and prevent hello flood attack. Nodes had been classified as friend and stranger based on the signal strength. Short client puzzles that require less computational power and battery power had been used to check the validity of suspicious nodes.

Sinkhole attack was among the most destructive routing attacks for WSNs. It may cause the intruder to lure all or most of the data flow that has to be captured at the base station. Routing protocol MintRoute was used to implement this attack. Once sinkhole attack has been implemented and the adversary node has started to work as network member in the data routing, it can apply some more threats such as, forwarding only the selective packets i. e. selective forwarding or dropping all the packets and forming a blackhole. Ultimately this drop of some important data packets can disrupt the sensor networks completely. Jatav *et al*, [15] presents a mechanism to launch sinkhole attack based attacks such as selective forwarding and balckhole attack in wireless sensor networks. The proposed work includes detection and countermeasure rules to make the sensor network secure from these attacks. It was observed through simulation that the proposed methods for detection and countermeasure achieve high degree of security with negligible overheads.

Chaudhari, *et al*, [16] made an effort to document all the known security issues in wireless sensor networks and discusses a wide variety of attacks in WSN and their classification mechanisms and different securities available to handle them including the challenges faced and took up the challenge and have proposed an integrated comprehensive security that will provide security services for all services of sensor network. The sensing technology combined with processing power and wireless communication makes it profitable for being exploited in great quantity in future. The wireless communication technology also acquires various types of security threats.

WSNs were susceptible to various attacks, in which Blackhole a kind of Denial of Service (DoS) attack was very difficult to detect and defend. In blackhole attack, an adversary captures and re-programs a set of nodes in the network to block the packets they receive instead of forwarding them towards the base station. As a result any information that enters the blackhole region was captured and doesn't reach the destination. Due to this attack, high end-to-end delay was introduced in the network and performance of the network (i.e. throughput) was degraded. Wazid *et al*, [17] proposed a comparative performance analysis of two WSN's topologies i.e. Tree and Mesh under blackhole attack was done. If there was a WSN prone to blackhole attack and requires time efficient network service for information exchange then Tree topology was to be chosen. If it requires throughput efficient and consistent service in the network then Mesh topology was recommended. An algorithm named as Topology Based Efficient Service Prediction (TBESP) algorithm has been proposed depending upon the analysis done which will help in choosing the best suited topology as per the network service requirement under blackhole attack.

Tripathi *et al*, [18] provides an overview of LEACH, the most popular clustered routing protocol of WSN and how LEACH can be compromised by Black hole and Gray Hole attacker. "High energy threshold" concept was used to simulate these attacks on NS-2. The performance of WSN under attack was thoroughly investigated, by

applying it on various network parameters with various node densities. It was observed that the effect of the Black Hole attack was more on the network performance as compared to the Gray Hole attack.

Sheela *et al*, [19] proposes a lightweight, fast, efficient and mobile agent technology based security solution against black attack for WSNs. WSN has a dynamic topology, intermittent connectivity and resource constrained device nodes. The proposed scheme was to defend against black hole attack using multiple base stations deployed in network by using mobile agents. A packet drop attack or black hole attack was a type of denial-of-service attack accomplished by dropping packets. The attack could be accomplished either selectively (e.g. by dropping packets for a particular network destination, a packet every n packets or every t seconds, or a randomly selected portion of the packets, which is called "Gray hole attack") or in bulk (by dropping all packets). Mobile agent was a program segment which is self-controlling. They navigate from node to node not only transmitting data but also doing computation. They were effective paradigm for distributed applications and especially attractive in a dynamic network environment. This mechanism does not require more energy. A simulation-based model of our solution to recover from black hole attack in a Wireless Sensor Network was introduced. Comparison of communication overhead and cost were made between the system without using multiple base stations and the system with multiple base stations to prevent black hole attacks. Comparison was also made between the proposed attack detection system using mobile agents against the security system in the absence of mobile agents. The mobile agents were developed using the Aglet.

Gondwal *et al*, [20] proposed a technique to detect the black-hole attack using multiple base-stations and a check agent based technology. This technique was Energy efficient, Fast, Lightweight and Reduces message complexity. An effective solution was proposed that uses multiple base stations to improve the delivery of the packets from the sensor nodes reaching at least one base station in the network, thus ensuring high packet delivery success. The proposed technique was more efficient than the previous techniques and gives better results. Check agent was a software program which was self-controlling and it moves from node to node and checks the presence of black-hole nodes in the network. Routing through multiple base stations algorithm was only activated when there was a chance of black-hole attack on the network.

Yadav *et al*, [21] presented a fuzzy based decision to check a node was infected by Black hole attack or node. The proposed system will identify the attack over the node as well as provide the solution to reduce the data loss over the network. The proposed method will first detect the black hole node using fuzzy rule. The fuzzy rule is implemented on response time of node communication. Now instead of transferring data on this node, it will be passing on from the surrounding nodes; it will only handle the transmission that is directed to it only. The proposed algorithm provides better solution for reducing the data loss over the network.

Dighe *et al*. [22] proposed an efficient technique that uses multiple base stations deployed in the network to reduce the impact of black holes on data transmission. The proposed method sends copies of data packets to these multiple base stations. The proposed solution is highly effective andrequires very little computation and message exchange in the network, thus saving the energy of the nodes. Simulation results prove that our scheme achieves the 99% packet delivery success and the 100% black hole node detection.

Zhang *et al*, [23] proposed a Hierarchical Role-based Data Dissemination approach, named HRDD, for large-scale WSNs with multiple mobile sinks. In HRDD, a hierarchical cluster-based structure to discover and maintain the routing paths for distributing data to the mobile sink and assign two roles, named Indexing Agent and Gateway Agent, to some sensor nodes in the wireless sensor networks. Indexing Agents were used to remove unnecessary query messages, while Gateway Agents contribute to decrease energy consumption and the broadcasting messages. The evaluation and compared the impact of the number of nodes with prior approach. The simulation results justify that HRDD has the capability to reduce the energy consumption in the wireless sensor networks and to prolong network lifetime.

Lin *et al*, [24] proposed a Hierarchical Cluster-based Data Dissemination scheme, named HCDD, to disseminate data to the mobile sink with light control overhead. In HCDD, the sensor nodes were self-organized to find the route without the knowledge of node's location information. That is, unlike other works, the HCDD can operate without any expensive and power-consuming GPS device used for estimating the location information. The simulation results shows that our HCDD scheme can greatly alleviate the control overhead and, at the same time, achieve longer network lifetime and comparable number of received data with previous works, such as the TTDD-like methods.

Shin *et al*, [25] proposed a stable backbone tree construction algorithm using multi-hop clusters for WSNs. The hierarchical cluster structure has advantages in data fusion and aggregation. Energy consumption could be decreased by managing nodes with cluster heads. Backbone nodes, which were responsible for performing and managing multi-hop communication, could reduce the communication overhead such as control traffic and minimize the number of active nodes. Previous backbone construction algorithms, such as HCDD and Multicluster, Mobile, Multimedia radio network (MMM), consume energy quickly. They were designed without regard to appropriate factors such as residual energy and degree (the number of connections or edges to other nodes) of a node for WSNs. Thus, the network was quickly disconnected or has to reconstruct a backbone.

A distributed algorithm to create a stable backbone by selecting the nodes with higher energy or degree as the cluster heads. This increases the overall network lifetime. Moreover, the proposed method balances energy consumption by distributing the traffic load among nodes around the cluster head. In the simulation, the proposed scheme outperforms previous clustering schemes in terms of the average and the standard deviation of residual energy or degree of backbone nodes, the average residual energy of backbone nodes after disseminating the sensed data and the network lifetime.

A large-scale data dissemination application was characterized by a large number of information flows and information consumers. Consumers were interested in different, yet overlapping, subsets of the flows. Multicast was used to deliver subsets of the flows to subsets of the consumers. Since multicast groups were a limited resource, each consumer must filter out a large number of unneeded flows. Tock *et al*, [26] proposed alleviate the end-node filtering load by using hierarchical clustering of flows to transport-layer sessions and clustering of sessions to network-layer multicast groups. This scheme allows for hierarchical filtering of flows at the receivers. Formulating a cost function that models and emphasizes the filtering process and propose algorithms for the solution of the hierarchical mapping problem. Performance evaluation indicates a significant reduction of end node filtering cost compared to a non-hierarchic approach.

Methodology: The Hierarchical Cluster-based Data Dissemination(HCDD) protocol [24] defines a hierarchical cluster architecture to keep the location of mobile sinks and and paths for the data dissemination from the sensors to the sink. Each cluster is composed by a cluster head, several gateways and ordinary sensors as seen in Figure 1 [27]. When a mobile sink crosses the network, it registers itself to the nearest cluster head. A notification message is then propagated to all cluster heads. During this procedure, each cluster head records the sink ID and its sender such that future data reports transmission can be easily performed from sources to sink. The main drawback of the backbone-based approach is the need to maintain the structure. In addition, the hot spot problem can occur as the traffic is concentrated over a group of cluster heads or leaders.

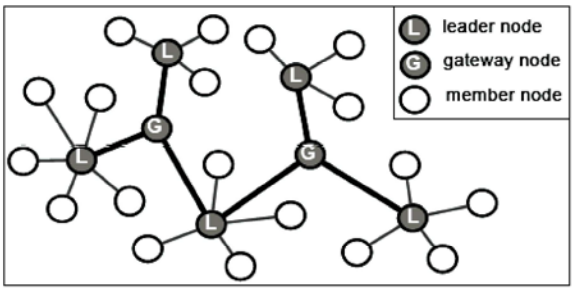

Fig. 1: Hierarchical Cluster-based Data Dissemination

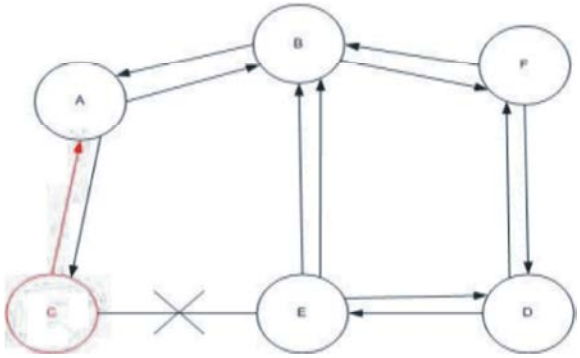

Fig. 2: Black Hole Attack

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address.

The method how malicious node fits in the data routes varies. Fig. 2 shows how black hole problem arises, here node "A" want to send data packets to node "D"

and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

Basic Definition

Definition 1: D_{AB} → Distance between two neighboring nodes (Say A & B).

$D_{AB} = (R-d) / V$

where R → Transmission range ; d→ Distance between Node A and Node B.
V → Average speed of the node.

Definition 2: Counter of agent

It tells how many times the agent finds the particular Node as a one hop neighbor or as a child node to the previous Node.

One mobile agent has agent ID, agent Program, agent briefcase (It contains some condition parameters such as D_{AB}, Counter, Latest location Claim of node it visited).

An agent is capable of sharing its briefcase with other agents and nodes. The state variables may be updated if necessary when an agent leaves a node.

Definition 3: Table details in every Node Counter of every node tells how many times this node has been visited by an agent. i.e., it represents frequency of the visits by agents.

Black Hole Attack Detection

Algorithm: Neighboring nods list is maintained by each node. Routing path is established using AODV Protocol. Initially routing is done through nearest base station i.e., without using multiple base stations.

Routing through multiple base station algorithm is activated only when there is a chance of black hole attack. This is needed to save the energy in WSN.

To check the probability of the presence of black hole nodes,

- Mobile agent randomly visits very node.
- When mobile agent visits a node i,
- it checks the frequency of receiving packets for every neighboring nodes in the list.
- if it finds '0' (No packet from node j to node i) for neighboring node j,
- it doubts node j is a black hole node.
- it triggers routing process algorithm through multiple base stations for time t.
- Within time t,
- it confirms whether node j is a blackhole node or not.
- if node j is a black hole node, it
- revokes node j.
- After time t, it triggers routing process algorithm through nearest base station.(without using multiple base stations)

RESULT AND DISCUSSION

In this work, the impact of black hole attack is observed in WSN. The experimental setup consists of 40 nodes distributed over 1.5 square kilometer. Hierarchical cluster-based data dissemination is used. Two experiments are conducted the first without malicious nodes and the second with 5% of the nodes being malicious. The malicious nodes are designed to randomly drop packets irrespective of the source or destination address. The attack simulated is Black hole attack. Figure 3 to Figure 5 show the network performance in terms of throughput, end to end delay and data dropped respectively. All the outputs plotted are in time average format [28].

The Figure 3 shows the results of the throughput for WSN with and without malicious nodes. The throughput decreases by an average of 34.27% in the presence of 5% malicious nodes.

It is observed from Figure 4, that the end to end delay increases by an average of 50.39% due to the black hole attack in WSN

In a black hole attack, the attacker swallows (i.e. receives but does not forward) all the messages he receives. As a result any information that enters the black hole region was captured. It is seen in Figure 5 that an average of 35.3% data packets are dropped or captured by the malicious nodes.

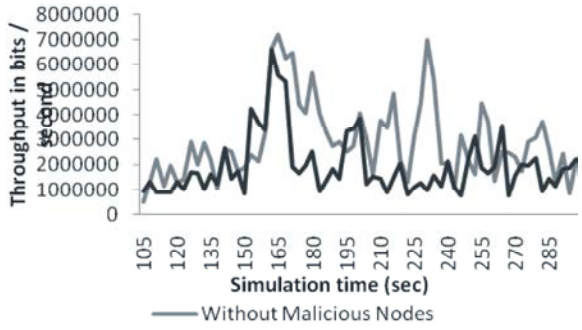

Fig. 3: Throughput

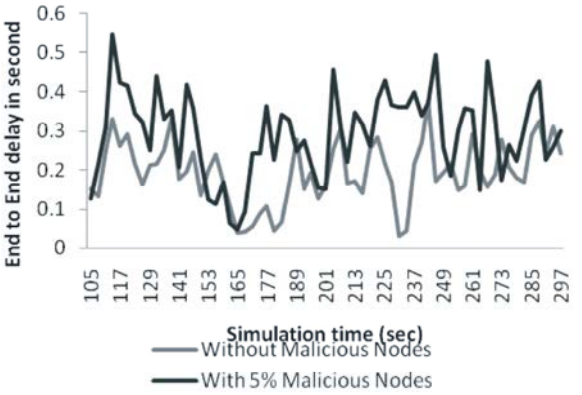

Fig. 4: End to End Delay

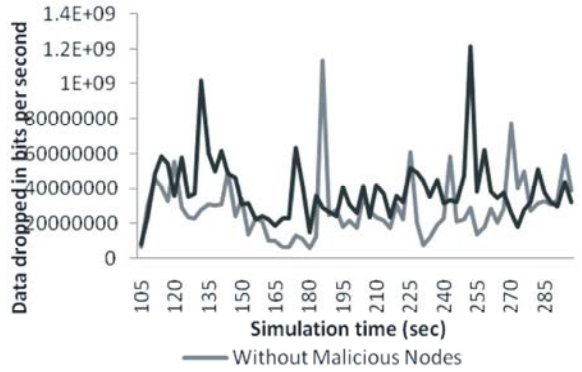

Fig. 5: Dropping of data

CONCLUSION

The significant advances of hardware manufacturing technology and the development of efficient software algorithms make technically and economically feasible a network composed of numerous, small, low-cost sensors using wireless communications, that was, a wireless sensor network. Sensor networks had great potential to be employed in mission critical situations like battlefields but also in more everyday security and commercial applications such as building and traffic surveillance, habitat monitoring and smart homes etc. However, wireless sensor networks pose unique security challenges. Security was becoming a major concern for WSN protocol designers because of the wide security-critical applications of WSNs.In this paper, it is proposed to evaluate the performance of a network under the impact of malicious nodes.The malicious nodes are designed to randomly drop packets irrespective of the source or destination address. The attack simulated is Black hole attack. Simulation results show that the throughput decreases by an average of 34.27% and data dropped increases by an average of 35.3% in the presence of 5% malicious nodes. Further investigations to identify malicious node and ways to mitigate them are critical.

REFERENCES

1. Sahni, S. and X. Xu, 2005. Algorithms for wireless sensor networks. International journal of distributed sensor networks, 1(1): 35-56.
2. Heinzelman, W.B., A.L. Murphy, H.S. Carvalho and M.A. Perillo, 2004. Middleware to support sensor network applications. Network, IEEE, 18(1): 6-14.
3. Han, K., L. Xiang, J. Luo, M. Xiao and L. Huang, 2013. Energy-efficient reliable data dissemination in duty-cycled wireless sensor networks. In Proceedings of the fourteenth ACM international symposium on Mobile ad hoc networking and computing ACM., pp: 287-292.
4. Vecchio, M., A.C. Viana, A. Ziviani and R. Friedman, 2010. DEEP: Density-based proactive data dissemination protocol for wireless sensor networks with uncontrolled sink mobility. Computer Communications, 33(8): 929-939.
5. Starobinski, D. and W. Xiao, 2010. Asymptotically optimal data dissemination in multichannel wireless sensor networks: Single radios suffice. Networking, IEEE/ACM Transactions on, 18(3): 695-707.
6. Jain, N., 2011. Energy Efficient And Cluster Based Routing Protocol For Wireless Sensor Network: A Review. International Journal of Advance Technology & Engineering Research, 1(1).
7. Singh, S.K., M.P. Singh and D.K. Singh, 2010. A survey of energy-efficient hierarchical cluster-based routing in wireless sensor networks. International Journal of Advanced Networking and Application (IJANA), 2(02): 570-580.
8. Mhatre, V. and C. Rosenberg, 2004. ìHomogeneousvs heterogeneous clustered sensor networks: a comparative studyî, Communications, 2004 IEEE International Conference on, pp: 6.

9. Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. Wireless sensor networks: a survey. Computer networks, 38(4): 393-422.
10. Padmavathi, D.G. and M. Shanmugapriya, 2009. A survey of attacks, security mechanisms and challenges in wireless sensornetworks. arXiv preprintar Xiv:0909.0576.
11. Karlof, C. and D. Wagner, 2003. Secure routing in wireless sensor networks: Attacks and counter measures. Ad hoc networks, 1(2): 293-315.
12. Papadimitratos, P. and Z.J. Haas, 2002. Securing the Internet Routing Infrastructure, IEEE Communications, 10(40): 60-68.
13. Ramaswamy, S., H. Fu, M.Sreekantaradhya, J. Dixon and K.E. Nygard, 2003. Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. In International Conference on Wireless Networks.
14. Singh, V.P., S. Jain and J. Singhai, 2010. Hello flood attack and its countermeasures in wireless sensor networks. International Journal of Computer Science, 7(3): 23.
15. Jatav, V.K., M. Tripathi, M.S. Gaur and V. Laxmi, 2012. Wireless Sensor Networks: Attack Models and Detection. In 2012 IACSIT Hong Kong Conferences, IPCSIT vol. 30 (2012)©(2012) IACSIT Press, Singapore.
16. Chaudhari, H.C. and L.U. Kadam, 2011. Wireless Sensor Networks: Security, Attacks and Challenges, International Journal of Networking, 1(1): 04-16.
17. Wazid, M., A. Katal and R.H. Goudar, 2013. TBESP algorithm for Wireless Sensor Network under Blackhole attack. In Communications and Signal Processing (ICCSP), 2013 International Conference on, IEEE, 1086-1091.
18. Tripathi, M., M.S. Gaur and V. Laxmi, 2013. Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN. Procedia Computer Science, 19: 1101-1107.
19. Sheela, D., V.R. Srividhya, Anjali Asthma Begam and G.M. Chidanand, 2012. Detecting Black Attacks in Wireless Sensor Networks using Mobile Agent.
20. Gondwal, N. and C. Diwaker, Detecting blackhole attack in wsn bycheck agent using multiple base stations.
21. Yadav, P., R.K. Gill, Kumar and N.A. Fuzzy, 2012. Based Approach to Detect Black hole Attack. International Journal of Soft Computing and Engineering (IJSCE) ISSN, 2231-2307, 2(3).
22. Dighe, P.G. and M.B. Vaidya, 2012. Deployment of Multiple Base Stations to Counter Effects of Black Hole on Data Transmission in Wireless Sensor Network. International Journal of Engineering and Innovative Technology, 1(4): 209-213.
23. Zhang Chun, FeiShumin, Exploiting mobility for data collection in Wireless Sensor Networks.
24. Lin, C.J., P.L. Chou and C.F. Chou, 2006. HCDD: hierarchical cluster-based data dissemination in wireless sensor networks with mobile sink. In Proceedings of the 2006 international conference on Wireless communications and mobile computing ACM, 1189-1194.
25. Shin, I., M. Kim, M.W. Mutka, H. Choo and T.J. Lee, 2009. MCBT: multi-hop cluster based stableBackbone trees for data collection and dissemination in WSNs. Sensors, 9(8): 6028-6045.
26. Tock, Y., N. Naaman, A. Harpaz and G. Gershinsky, 2005. Hierarchical Clustering of with delay reduction, Control conference (CCC), 2011 30th chinese, 44 July 2011, Message Flows in a Multicast Data Dissemination System, In IASTED PDCS, 22-320-326.
27. Hamida, E.B. and G. Chelius, 2008. Strategies for data dissemination to mobile sinks in wireless sensor networks. Wireless Communications, IEEE, 15(6): 31-37.
28. Tripathi Meenakshi, M.S.Gaur and V. Laxmi, 2013. Malaviya National Institute of Technology, Jaipur, India, : Evaluation Of Performance Degradation Due To Black Hole Attack In Wireless Sensor Networks, The 8th International Symposium on Intelligent Systems Techniques for Ad Hoc and Wireless Sensor Networks (IST-AWSN), Elsevier Sciverse Science Direct Procedia Computer Science, 19: 1101-1107.