Analysis of Various Attacks in Routing Protocols for Wireless Sensor Network

Muhammad Danish Qureshi, Hassam Ishtiaq, Arsalan Farhat, Obaid Rehman

Abstract— Demand of wireless sensor network is increasing for various smart applications and provides unlimited opportunities. But with the increase in usage of WSN it imposes some challenges including limited power resources and security threats which needs to be identified and its mitigation techniques requires further development. In this paper we analyzed different routing protocols including SEER, Direct Diffusion, Tiny OS Beaconing, Geographic routing and Rumor Routing and its various attacks on these routing protocols. Our work also analyzes the design issues of WSN by comparing different design parameters including power usage, scalability, data aggregation, overhead, fault tolerance and quality of service. After analysis of these protocols we present its comparison which shows the important features required for consideration while suggesting routing protocols for WSN. Furthermore, as a result optimum protocol is suggested in term of security and its energy efficiency.

Index Terms— Design parameter, Evasdropping, QOS, Routing protocol, Sybil attack, Wormhole, WSN.

1 Introduction

Wireless sensor network is consisting of different nodes that maintain a cooperative network. Every node has RF (Radio Frequency) transceiver, power source, various sensors and actuators and processing capabilities. Nodes transmit and receive data wirelessly and it can automatically self organized into Ad hoc fashion after spreading into network. WSN is a need of smart environment that wants information about its internal work and about surrounding. This step includes in building, home, industrial and shipboard and transport systems automation. There are many applications of WSN in real world. It can be implemented for environment monitoring, for military operation, in factories for maintenance, health monitoring and even in bodies of patient. As every network need a routing protocol for implementation and running of network, WSN also has some routing protocols. Routing in WSN is different from routing in other ordinary networks. In WSN there is infrastructure, wireless links are unreliable that may fail, routing protocols of WSN have to meet strict energy saving and security requirements [1], [2], [7].

2 Attacks in WSN

2.1 Eavesdropping

WSN uses broadcast nature, so an attacker having strong receiver can intercept and eavesdrop data. It can attract data like location of node, Node ID, Message ID etc [12].

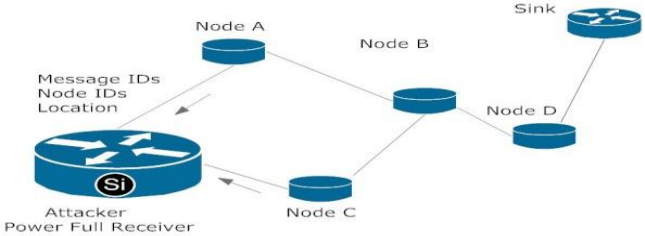

Fig. 1 Eavesdropping

2.2 Denial of service (DOS)

Attacker wants to disrupt, corrupt or destroy a network. Its task is to jam a node or set of nodes. It simply transmits radio signals that create interference with the radio frequency used by the network [13].

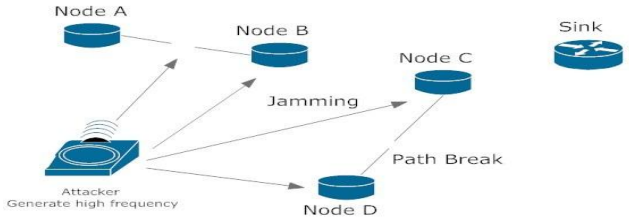

Fig. 2 DOS

2.3 Message tampering

Attacker receives the message and then forwards it to other node after tempering it. So when data reaches to the sink is not useful [13].

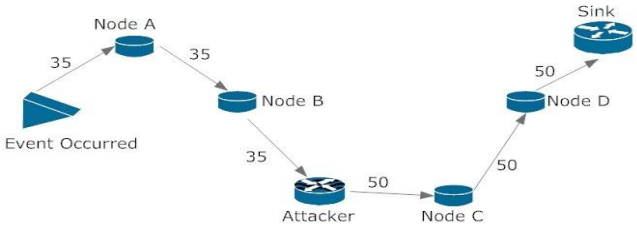

Fig. 3 Message tempering

2.4 Selective forwarding

Attacker node receives the message but it refuses to forward it and simply drop it, ensuring that the message cannot be propagate further. Attacker acts like a hole and don't forward packet [13].

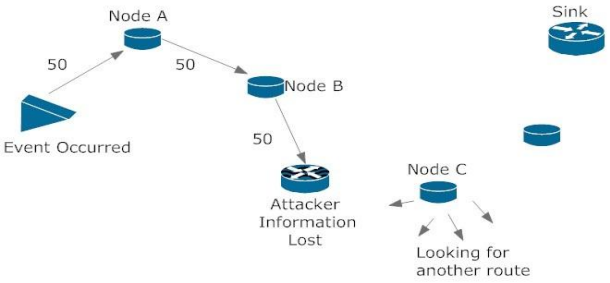

Fig. 4 Selective forwarding

2.5 Sinkhole attacks

Attacker is very powerful in this attack. It attracts all the nodes from a particular area and creates itself as a sink for other nodes. Now it can change the data as well as drop it. It also leads to the other attacks [14].

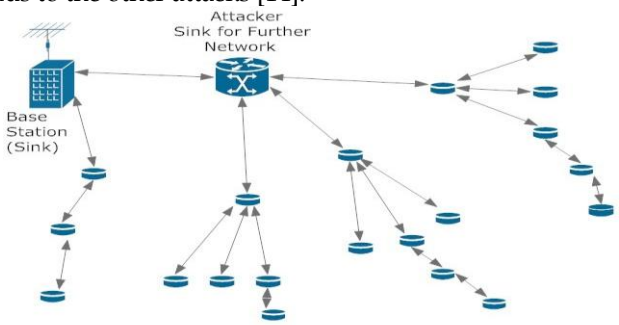

Fig. 5 Sinkhole attacks

2.6 Wormhole attacks

Attacker receives the information by making a path of low latency link between two different parts of the network. It forwards the message of one part to other part for making confusion. It also allows sinkhole to occur as the attacker on other side of the wormhole can shows to have a high quality path to the sink. An attacker that is located near to the sink may completely disrupt routing by creating a best location wormhole [13].

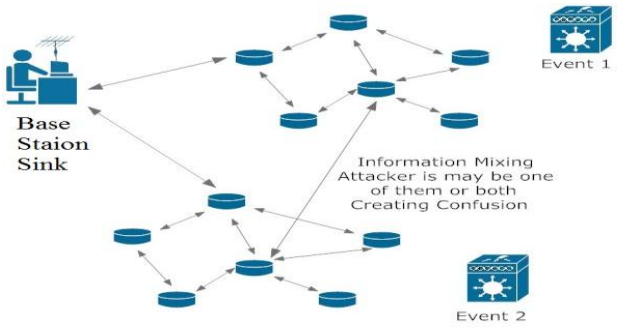

Fig. 6 Wormhole attacks

2.7 Sybil attacks

Attacker shows multiple identities to other nodes in the network. It can decrease the effectiveness of fault tolerant such as storage distribution, disparity and multi path routing, and maintenance of topologies. By multiple identities it makes such a condition that every message should be go through that attacker [13].

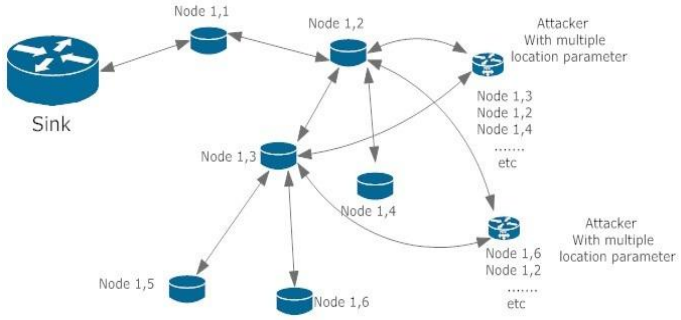

Fig. 7 Sybil attacks

3 Design Parameters

Following are the some design parameters which has much importance while suggesting a protocol:

3.1 Fault Tolerance

Sensor nodes have much chances of failure due to odd and difficult deployment environments. Thus, sensor nodes should have ability of fault tolerant and have the abilities of testing themselves, auto celebrate, auto repair and self recovering [3].

3.2 QoS support

In WSN, every application may have different quality of service (QoS) requirements in terms of delivery latency path and packet loss. Network protocol design should consider the QoS requirements of applications [3].

3.3 Power consumption

Sensor nodes use the battery for power and it is very difficult to charge or recharge their batteries, so it is very important to control and reduce the power consumption of nodes so that the lives of the sensor nodes increases, as well as the network will live for longtime [5].

3.4 Scalability

The sensor nodes in WSN are in the order of tens, hundreds,

- *Muhammad Danish Qureshi is currently pursuing bachelor degree* program *in electric engineering in Sarhad University of Science & IT, Pakistan, PH-+923333633945. E-mail: mdanishqureshi@yahoo.com*
- *Hassam Ishtiaq, Arsalan Farhat, Obaid Rehman is currentlyaffiliated with Sarhad University of Science & IT, Pakistan.*

or thousands, routing protocols designed for sensor networks should be scalable to different network sizes [5].

3.5 Reliability

Routing protocols designed for WSN must have error control and correction functions to ensure reliability of data delivery over noise and time varying channels [3].

3.6 Channel Utilization

WSN have limited bandwidth resources. Routing protocols designed for sensor networks must use the whole bandwidth very efficiently to improve channel utilization [5].

3.7 Overhead

Overhead is also a special design parameter. In many cases overheads are not allowed. Overhead may be in form of bandwidth, space area, large number of nodes etc [3].

4 Routing Protocols

There are 7 major types that includes (1) Centric Protocols (2)Hierarchical Protocols (3)Location based Protocols (4)Mobility Based Protocols (5)Multi path based Protocols (6) Heterogeneity based Protocols (7) QoS based Protocols. In next section we will study some of the routing protocols of WSN and compare them on the basis of security and design parameters. We will compare the following protocols:

- SEER (Data centric, Location based)
- Directed Diffusion (Data centric)
- TinyOS beaconing (Hierarchical)
- Geographic routing (Location based Protocols)
- Rumor Routing (Data centric)

4.1 SEER (Secure and Energy Efficient Multi Path Routing Protocol)

SEER uses multi paths between two nodes one by one to increase the life of the network. Multi path specially uses for two functions. One is for balancing of load and the other is for making data delivery reliable. The sink first broadcasts a ND (Neighbors Discovery) packet to the network. The sink broadcasts another packet NC. Information about nodes is collected during the previous broadcasting (Energy levels of the node etc) [18], [19].

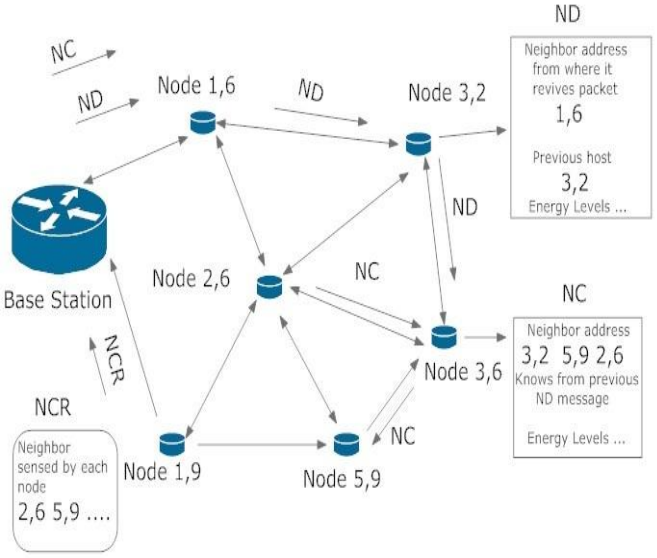

Fig. 8 SEER Operation

When node gets the NC message, it replies a NCR packet to the sink. The NCR packet has the location and the information about the node and the list of all addresses of its neighbor nodes. Path is only selected by the sink only. Base Station or sink select different paths after a certain period according to current energy level of node. This gives the surety that if the attacker advertises; it has no affect on path selection process. After the sink selects another path, the attacker cannot attack any more [17].

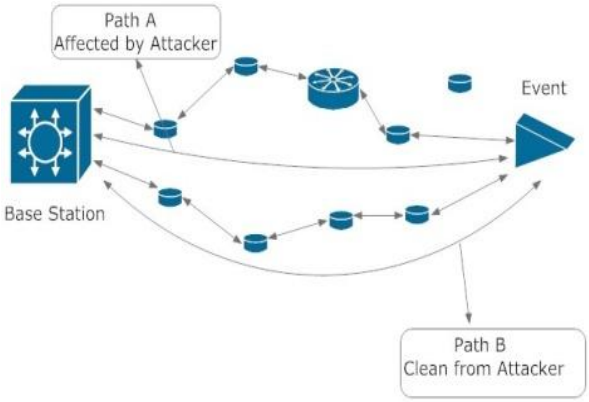

Fig. 9 SEER defending

4.2 Directed Diffusion

Directed Diffusion is a type of data centric protocol for communicating data in sensor network. Here if base station wants data he has to first broadcast interest packet. An interest packet is a request that should be done by the base station. Every node keeps moving with that interest packet until that packet reaches to the node that is interested or satisfies the interest condition. Each node that gets the interests packet set up a slope value toward the origin node. A slope value contains direction and attributes value. As shown in Figure when node

"B" gets an interest packet from node "A", it includes "A (Δ)" in its slope value. Similarly when node "C" receives an interest from node "A" and node "D", it includes "B (2Δ)" and "D (2Δ)". When interest packet reached to the place of event, then the sink strictly forces one or more neighbor's nodes to reply at a higher data rate. Also sink can negatively force the nodes to leave high data flow that are not in use at that event [15], [10].

In that scenario attacker can eavesdrop the interest. After an attacker gets an interest packet from a sink, it can simply reply with the message that "I am the node that is interested". When the reply for that interest is sent, then after sink the attacker would also be receiving them.

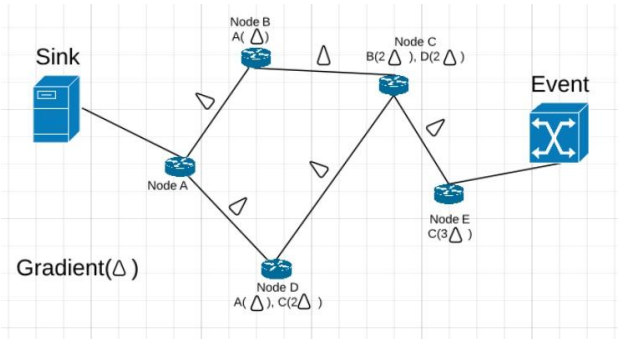

Fig. 10 Directed Diffusion

When source generate data events, an attacker node can attack a data flow and cause to suppression. It is denial of service attack.

4.3 TinyOS beaconing

It is a hierarchical Protocol. It builds a tree with a sink as the parent for all the other nodes in the sensor network. After a certain period the sink always broadcasts new route information to the neighbor nodes, nodes that receives that information also forward it to their neighbors. Nodes that get the new route path information mark the sink as its parent and rebroadcast the update [14].

That is a very simple protocol that makes it so much susceptible to all the attacks discussed above. Since new routing path information are not authenticated, so an attacker can easily say that or claim himself as a parent of the all other nodes of sensor network. An attacker who is interested in eavesdropping or suppressing packets in a particular area can easily do it by creating a combination of wormhole or sinkhole attack [14], [6].

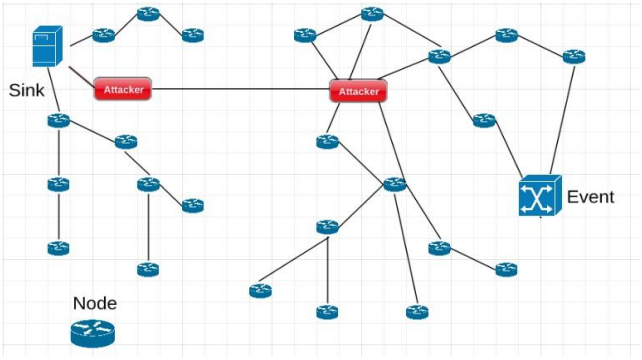

Fig. 11 TinyOS beaconing

4.4 Geographic Routing

GEAR (Geographic and Energy Aware Routing) use nodes location addresses to inform node that is near to it about interest and also express geographic message destinations to efficiently propagate queries and route replies in the WSN. A black hole is created when there is no further node near to the event other than it. Whenever a message is received by a node it checks the nearby node that is closest to the target. If there is more than one node, then it will choose that is much closer to the target [6], [9].

And if there is only one node it forwards the packet to that node. If there is no node near to that, then it will choose the node using a function known from above, that this protocol uses location and energy levels information. In this protocol an attacker can increase his strength of attack by creating a Sybil attack. Attacker can create Sybil attack by covering up the target node and its path totally by number of compromising nodes [13].

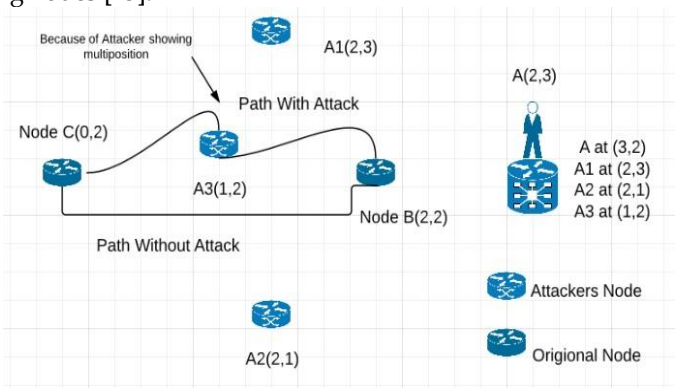

Fig. 12 Geographic routing

As shown in figure that an attacker "A" have actual address of location (3, 2) also advertized some fake locations that actually not exists (i.e. A1, A2 and A3). Now if "B" wants to communicate with node "C" at (0, 2) it will communicate through "A3" because of fake advertisement. So that type of communication is an overhead that is handled by an attacker. Attacker can easily do selective forwarding here [14].

4.5 Rumor Routing

Rumor routing is such a protocol that actually intersects the paths of queries and data events. It is very efficient at the situation where high flooding is not possible. It does not allow the whole network to match or found the event (interest). Rumor routing uses a healthy living message or packet knows as AGENT. Source node generates an agent whenever it observes an event. Agent propagates along the whole network and forwards the information about the event and remote nodes [16], [11].

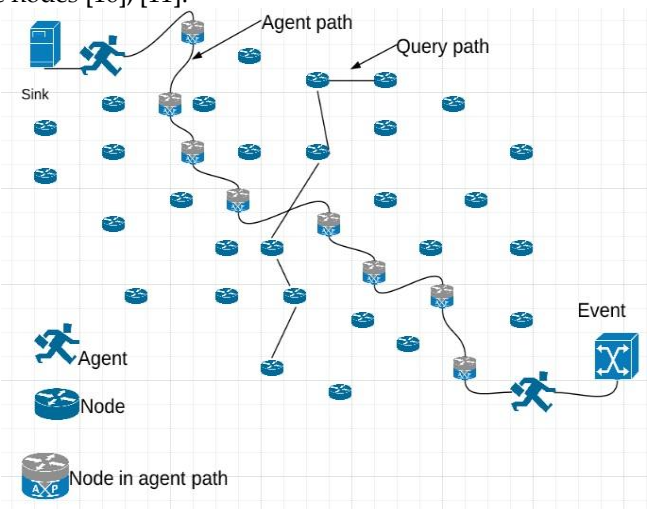

Fig. 13 Rumor Routing

Agent have the information like list of events, hope path to the event, list of nodes from which it is coming and a TTL (Time to Live) field. When it reaches to new node it actually tells the node about the event and adds that node in an event list. It also decreases the TTL field by one at every new node visit. Now if TTL field is more than zero it selects the agent's next hope from its neighbors in the table and subtracts the previously visited node from table. Similarly sink or base station creates an agent to propagate the queries into network. So a point comes when both the paths (i.e. queries path and data event path will intersect) is our desired point. After that a final path is decided for communication between event and base station [15], [16].

5 Comparison on the Basis of Security and Design Parameters

After studying different protocols deeply we analyze that there is no such a protocol that gives 100% surety of security. But there are some protocols that are secure enough from other protocols. Below are the tables of comparision of routing protocols on the basis of attacks and design parameters.

TABLE 1
COMPARISION ON THE BASIS OF ATTACKS

Routing Protocol	Eavesdropping	Denial of service	Message Tampering	Selective Forwarding	Sinkhole Attacks	Wormhole Attacks	Sybil Attacks	Hello Attacks
SEER	Yes	Yes	Yes (Only for first time)	Yes (Only for first time)	Yes	Less Chance	No	No
Direct Diffusion	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TinyOS Beaconing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Geographic Routing	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Rumor Routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

[5], [6], [18], and Analysis

TABLE 2
COMPARISION ON THE BASIS OF DESIGN PARAMETERS

Routing Protocol	Classification	Power Usage	Data Aggregation	Scalability	Overhead	Data Delivery Model	QOS	Fault Tolerance
SEER	Data centric/ Location	Low	No	Yes	Low	Demand driven	Yes	Good
Direct Diffusion	Flat/ Data centric	Limited	Yes	Limited	Low	Demand driven	No	No
TinyOS Beaconing	Hierarchical	High	Yes	Good	High	Demand driven	No	No
Geographic Routing	Location	Limited	No	Limited	Low	Cluster head	No	Good
Rumor Routing	Flat/ Data centric	Low	Yes	Good	Low	Demand driven	No	Good

[6], [20] and Analysis

6 Conclusion

After studying deeply these five protocols we realize that SEER is a best protocol for security as well as energy efficiency as compared to other routing protocols, As in SEER, the path is changing continuously for next transmission. So it monitors each nodes energy level and position. If attackers wants to take control on network then there should be number of attackers are required to create a path between sink and event. After comparing in both cases security and design parameters we conclude that SEER is the best in both cases. SEER is actually created for energy efficiency but it also gives best security.

Acknowledgments:

In the name of Allah, the Most Gracious and the Most Merciful Alhamdulillah, all praises to Allah for the strengths and His blessing in completing this research paper. After that I would like to thanks my beloved parents "Izhar Ahmad Qureshi" who supported me alot. My work is also supported by my supervisor "Obaid Rehman" and "Sarhad University of Science & IT".

References:

[1] John A. Stankovic, "Wireless Sensor Networks", Department of Computer Science University of Virginia Charlottesville, Virginia 22904, June 2006.

[2] F. L. LEWIS, Associate Director for Research, "Wireless Sensor Networks1", The University of Texas at Arlington 7300 Jack Newell Blvd. S Ft. Worth, Texas 76118-7115 August 2009.

[3] Kay Romer and Friedemann Mattern, "The Design Space of Wireless Sensor Networks" IEEE Wireless Communications, pp. 54-61, December 2004.

[4] John Paul Walters et al, A Survey: "Wireless Sensor Network Security", Department f Computer Science Wayne State University, August 2008.
[5] Shio Kumar Singh, M P Singh et al, A Survey: "Routing Protocols in Wireless Sensor Networks", Maintenance Engineering Department Jamshedpur, Jharkhand, India, 2011.
[6] S.K. Singh, M.P. Singh and D.K. Singh, "A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks", International Journal of Advanced Networking and Application (IJANA), vol. 02, issue 02, pp. 570–580, October 2010.
[7] S. Misra et al, "Guide to Wireless Sensor Networks, Computer Communications and Networks", DOI: 10.1007/978-1-84882-218-4 4, Springer Verlag London Limited, 2009.
[8] E. Zanaj, M. Baldi, and F. Chiaraluce, "Efficiency of the Gossip Algorithm for Wireless Sensor Networks", In Proceedings of the 15th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split–Dubrovnik, Croatia, September, 2007.
[9] Yu, R. Govindan, and D. Estrin, "Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks", Technical Report UCLA/CSD-TR-01-0023, UCLA Computer Science Department, May 2001.
[10] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks", Proceedings ACM MobiCom'00, Boston, MA, pp. 56-67, August 2004.
[11] D. Braginsky and D. Estrin, "Rumor routing algorithm in sensor networks", Proceedings ACM WSNA, in conjunction with ACM MobiCom'02,Atlanta, GA, pp. 22-31, Sept. 2002.
[12] J. Yick, B. Mukherjee and D. Ghosal "Wireless Sensor Network Survey", Computer networks, Vol. 52, no. 12, pp 2292- 2330, 2008.
[13] R. El-Kaissi, A. Kayssi, A. Chehab, and Z. Dawy., DAWWSEN: "A Defence mechanism Against Wormhole attacks in Wireless Sensor Networks", 2009.
[14] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berkeley, 2010.
[15] S. Shanmugham, "Secure Routing in Wireless Sensor Networks" Scholarly Paper Advisor: Dr. Jens-Peter Kaps, 2011.
[16] D. Braginsky and D. Estrin, "Rumour routing algorithm for sensor networks", in First ACM International Workshop on Wireless Sensor Networks and Applications, 2002.
[17] Ch. Phani kanth and Pardhav Lingam, "Secure Routing Protocols in Wireless Sensor Networks", Software Developer Technology, Guntur University, India, 2008.
[18] Nidal Nasser and Yunfeng Chen, "Secure Multipath Routing Protocol for Wireless Sensor Networks", ICDCSW 07 Proceedings of the 27th International Conference, 2006.
[19] Hancke, GP & Leuschner, CJ 2007, "SEER : a simple energy efficient routing protocol for wireless sensor networks", South African Computer Journal, vol. 39, pp. Dec 2007.
[20] Rajashree. V. Biradar and V.C. Patil "Special Issue on Ubiquitous Computing Security Systems", UbiCC Journal Volume 4,. May 2011.