# Simulation of a Secure Efficient Dynamic Routing In Wireless Sensor Network

**Shobha.K, Mamatha Jadhav.V**

***Abstract***— ***Wireless Sensor networks have features like low cost, flexibility, fault tolerance, high sensing fidelity, creating many new and exciting application areas for remote sensing. So, wireless sensor network has emerged as a promising tool for monitoring the physical world with wireless sensor that can sense, process and communicate. There are many issues of wireless sensor network which need to be addressed .So took up one of the idea to use OSPF for secure efficient dynamic routing in wireless sensor network. The protocols that are being used till date are not efficient enough in matter of the time taken for the transferring the message from one node to another. So this project provides secure efficient dynamic routing in wireless sensor network. The protocols that are being used just provide a data packet transfer without any proper time. With the implementation of open shortest path first protocol we can get a better routing path for with least cost path. Thus the implementation of this can give a better view in the data packet transferring.The Simulation of Secure Efficient Dynamic Routing in Wireless sensor network has been implemented using dijkstra's algorithm for finding shortest path between the nodes. For providing security to the messages DES algorithm is used. The messages are encrypted and decrypted using this algorithm in order to provide security. User can be able to create number of nodes in the network. User can be able to send the packets using shortest path so that it reaches fast. User can also able to view the Routing Table at each node. User can also be able to view different nodes placed with their Node location and Node id. So from the Implementation it can be conclude that the proposed technique is very cost effective, secure and simpler to configure. From the performance Analysis it is clear that OSPF Routing in Wireless Sensor Networks is Very cost effective and more number of packets can be sent.***

***Index Terms***— ***Open Shortest Path First (OSPF), Link-State Packets, Backbone Area of OSPF, Area Border Routers (ABRs).***

## I. INTRODUCTION

Wireless Sensor networks have features [1][15] like low cost, flexibility, fault tolerance, high sensing fidelity, creating many new and exciting application areas for remote sensing. So [2], wireless sensor network has emerged as a promising tool for monitoring the physical world with wireless sensor that can sense, process and communicate. There are many issues of wireless sensor network which need to be addressed [2]. As researchers are working in the area of wireless sensor network, more and more data is collected, the refined the models and techniques will become in the future. On the Internet [3] and other infrastructure networks, there is a clear separation of roles: there are end systems (nodes) and intermediate systems (routers, switches and the like).

But in sensor networks each node is potentially a router for some other nodes. This creates an entirely new set of vulnerabilities in the network layer. For example, routers can become neglectful, in that they selectively do not forward packets from other nodes, or they can become selfish, in the sense that they prefer to give preference to their own packets. Such behaviors are often the result of denial-of-service attacks. A WSN consists of an array of sensors [4], interconnected by a wireless communication network. Sensor data is shared between these sensor nodes and used as input whose function is to extract the relevant information from the available data. Main objectives of sensor networks include reliability, accuracy, flexibility, cost effectiveness and ease of deployment. Each node [3] has one or more sensing unit. All nodes in the sensor network act as information sources, sensing and collecting data samples from their environment. The main components [5] of sensors consist of a sensing unit, a processing unit, a transceiver, and a power unit. As with the popularity of wireless networks, importance of sensor networks has grown .Wireless sensor networks have a lot in common with wireless ad hoc networks, but many of the security mechanisms designed for ad hoc networks simply won't fly on networks of sensors. Unlike in ad hoc networks, not every pair of nodes in a sensor network needs to communicate. Also, in ad hoc networks many security mechanisms usually rely on public key algorithms, which are sometimes too expensive in terms of resources for sensor networks. We could attempt to adapt a secure routing protocol based on secret-key cryptography, but it would impose non-trivial packet overheads in addition to necessitating the gathering of node state information. Routing is the one which shows path to the packets. Routing[6] misdirection is an attack whereby malicious nodes advertise false routes to either inject artificial traffic into the channel, direct traffic to a fraudulent base station or node, eliminate part of the network by overtaxing its resources or avoid forwarding packets entirely. Such an attack can be foiled using authentication, network monitoring and redundancy techniques. Authentication mechanisms based on distributed certification authorities have been proposed, but these have been shown to be tough to implement in real-world environments. Some network monitor applications can have neighbor nodes listen to both the sender and forwarder of a message, and notify the sender if the exact packet is not forwarded to the next hop of the route within a specific time limit.

**Manuscript published on 30 June 2013.**
* Correspondence Author (s)

**Mrs.Shobha. K,** P.G Student Department of Computer Science at MSRIT Bangalore, INDIA .Presently doing IIIRd Sem M.Tech in Computer Science and Engineering at MSRIT,Bangalore,INDIA.

**Prof.. Mamatha Jadhav. V,** Assistant Professor Department of Computer Science at MSRIT Bangalore, INDIA.

Unfortunately, packet comparison is not enough, since aggregation points may delay transmissions until enough information has been collected. Even if the time threshold is long enough, aggregated data will probably not match transmitted data. This will result in mischaracterizing the aggregation node as a “bad actor.”

### *1.1 Battery Attacks*

Attacks [3] targeting the battery exhaustion of nodes are termed attacks on “system lifetime” [9].Why would an attacker bother? Suppose, for example, a sensor network is deployed as an early-warning system for biological or chemical attacks. Because of the widely distributed nature of the sensor network, it would be almost impossible for a terrorist to physically destroy it. An easier option would perhaps be to insert a few misbehaving nodes that force the legitimate sensors to work continuously until their batteries are totally exhausted. Then the terrorist [9] could proceed with his real-world attack, undetected. There is a difficult trade-off in the case of sensor networks. These devices [3] have a triple role: as data collectors, processors and forwarders. The resource constraints common to wireless sensor networks often deprive the security architect of one of our favorite tools: public key cryptography. Fortunately, even the “lowest” [10] modern sensors are getting better processors and more memory, enabling them to “speak IP” and participate in the global public key infrastructure. Good work, too, has been done on optimizing and miniaturizing public key algorithms, and elliptic curve approaches can sometimes work well. When memory is just too tight, or processors just too weak, however, clever work-around and hard compromises are needed.

## II. RELATED WORK

### *2.1 Existing System*

There is no security for wireless networks Wireless Sensor Networks (WSNs) are rapidly emerging as an important new area in wireless and mobile computing research.OSPF used for the wired network, for router to learn the routes dynamically. Applications of WSNs are numerous and growing, and range from indoor deployment scenarios in the home and office to outdoor deployment scenarios in adversary's territory in a tactical battleground. For military environment, dispersal of WSNs into an adversary's territory enables the detection and tracking of enemy soldiers and vehicles. For home/office environments [11], indoor sensor networks offer the ability to monitor the health of the elderly and to detect intruders via a wireless home security system. In each of these scenarios, lives and livelihoods may depend on the timeliness and correctness of the sensor data obtained from dispersed sensor nodes. As a result, such WSNs [11] must be secured to prevent an intruder from obstructing the delivery of correct sensor data and from forging sensor data. To address the latter problem, end-to-end data integrity checksums and post-processing of senor data can be used to identify forged sensor data. The focus of this is on routing security in WSNs. Most of the currently existing routing protocols for WSNs make an optimization on the limited capabilities of the nodes and the application-specific nature of the network, but do not any the security aspects of the protocols. Although these protocols [6] have not been designed with security as a goal, it is extremely important to analyze their security properties. When the defender has the liabilities of insecure wireless communication, limited node capabilities, and possible insider threats, and the adversaries can use powerful laptops with high energy and long range communication to attack the network, designing a secure routing protocol for List of various application [7] areas of WSN are as follows.

1. Military Situation Awareness
2. Battlefield Surveillance
3. Communication, Command,
4. Control, Targeting Systems
5. Fish Monitoring

Routing is the one which shows directions to the packets. It is the act of moving information across an internetwork from a source to destination. In other words, it is the process of selecting paths in a network along which to send network traffic. Routing, in a more narrow sense of the term, is often contrasted with bridging in its assumption that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a single routing table entry to represent the route to a group of devices. In large networks, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging). Routing has become the dominant form of addressing on the Internet. Bridging is still widely used within localized environments. Routing involves two basic activities.

1. Determining optimal routing paths
2. Transporting information groups.

Routing in wireless sensor network is as shown in the figure below.

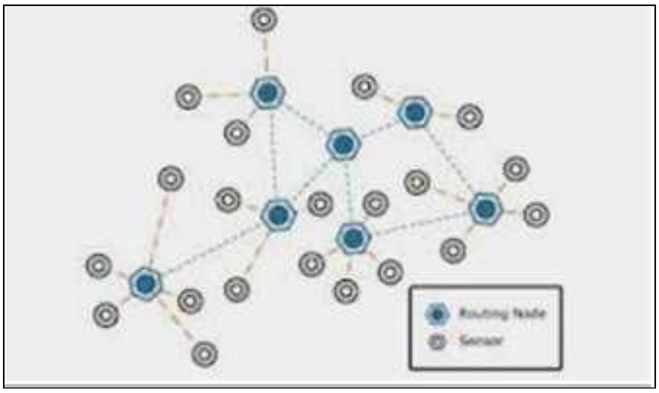

Figure 1: Routing in Wireless sensor Network

***Types of Routing***

- Static Routing-a route that is manually configured on the router
- Dynamic Routing-routes that a router learns by running a routing protocol

***Routing Techniques***

Here are the some of the Routing techniques listed below

- Adaptive routing
- Alternative-path routing
- Deflection routing
- Edge Disjoint Shortest Pair Algorithm
- Dijkstra's Algorithm
- Fuzzy routing
- Geographic routing
- Hierarchical routing
- Multi-path routing

*Published By:*
*Blue Eyes Intelligence Engineering*
*and Sciences Publication (BEIESP)*

***Routing Table***

A routing table is used by network routers to calculate the destinations of messages it is responsible for forwarding.

There are two basic methods of building a routing table:

- Static Routing Table
- Dynamic Routing Table

Static routing table is created, maintained, and updated by a network administrator, manually. A static route to every network must be configured on every router for full connectivity. This provides a granular level of control over routing, but quickly becomes impractical on large networks. Routers will not share static routes with each other, thus reducing CPU/RAM overhead and saving bandwidth. However, static routing is not fault-tolerant, as any change to the routing infrastructure (such as a link going down, or a new network added) requires manual intervention. Routers operating in a purely static environment cannot seamlessly choose a better route if a link becomes unavailable.

Dynamic routing table is created, maintained, and updated by a routing protocol running on the router. Examples of routing protocol OSPF (Open Shortest Path First).Routers do share dynamic routing information with each other, which increases CPU, RAM, and bandwidth usage. However, routing protocols are capable of dynamically choosing a different (or better) path when there is a change to the routing infrastructure.

### *2.2 Routing Protocols*

Routing protocols were created for routers. These protocols have been designed to allow the exchange of routing tables, or known networks, between routers. There are a lot of different routing protocols, each one designed for specific network sizes, so I am not going to be able to mention and analyze them all, but I will focus on the most popular. The two main types of routing: Static routing and Dynamic routing Routed Protocols. We all understand that TCP/IP, IPX-SPX are protocols used in a Local Area Network (LAN) so computers can communicate between with each other and with other computers on the Internet. Chances are that in your LAN you are most probably running TCP/IP. This protocol is what we call a "routed" protocol. The term "routed" refers to a protocol that contains specific type of information that allows it to be passed on from one network to another. In the example of TCP/IP, this protocol contains the destination IP Address to which the packet is destined to go, therefore you can construct a data packet and send it across to another computer on the Internet. Wireless Sensor network were first implemented in Military areas. Now a day's large range of applications of sensor network has become integral part of our life. Static routing allows routing tables in specific routers to be set up by the network administrator. Dynamic routing uses Routing Protocols that dynamically discover network destinations and how to get to them. Dynamic routing allows routing tables in routers to change if a router on the route goes down. Examples of Routing Protocols are AODV, EIGRP and OSPF. There are three basic types of routing protocols. Distance-vector Routing Protocols: Distance-vector Routing Protocols use simple algorithms that calculate a cumulative distance value between routers based on hop count. Example: RIP. Link-state Routing Protocols: Link-state Routing Protocols use sophisticated algorithms that maintain a complex database of internetwork topology. Example: OSPF Hybrid Routing Protocols: Hybrid Routing Protocols use a combination of distance-vector and link-state methods that tries to incorporate the advantages of both and minimize their disadvantages. Example: EIGRP.

## III. PROPOSED SYSTEM

***Open Shortest Path First* (OSPF)**[8][1] is a link-state routing protocol that was developed for IP networks and is based on the Shortest Path First (SPF) algorithm. OSPF is an Interior Gateway Protocol (IGP). We propose[to Develop[1] & simulate a secure efficient dynamic routing using protocol for the wireless sensor network Efficiency is an important factor because the sensor networks devices are energy constrained and may not charged again after drained, so the routing protocol should not consume more energy and drain the sensor nodes energy. We propose to use the OSPF routing protocol for the wireless sensor network.OSPF routing is previously used for the wired network, for router to learn the routes dynamically. We propose the way to use OSPF for the wireless sensor network. Each network node updates the link information to their neighbors and based on this link information, the route is learnt.Simulate the Established secure efficient routing protocol for the wireless sensor network using simulator.

In an OSPF network, routers or systems within the same area maintain an identical link-state database that describes the topology of the area. Each router or system in the area generates its link-state database from the link-state advertisements (LSAs) that it receives from all the other routers or systems in the same area and the LSAs that itself generates. An LSA is a packet that contains information about neighbors and path costs. Based on the link-state database, each router or system calculates a shortest-path spanning tree, with itself as the root, using the SPF algorithm. wireless sensor network. In the control plane, a routing protocol, e.g., BGP, OSPF, exchanges routing state updates and enables routers to compute the best paths towards various destinations. During this phase, an attacker can modify or inject malicious control messages leading to incorrect computation of routing paths. In the data plane, the routers forward the data along the paths computed in the control plane. Even if an attacker is not successful during the control phase, he can choose not to use the correct routing paths and forward data along routes that benefit him. Research shows that, attacks on the control plane can be mitigated by ensuring message integrity and, attacks on the data plane can be mitigated by ensuring route integrity. Earlier works have addressed these two problems independently with many interesting solutions. However, due to the nature of these solutions, network architects cannot deploy security at both planes without increasing the overhead on the network. This paper mainly concentrates on that. For Routing purpose we can use many standard protocols available. Especially for dynamic routing OSPF can be used in order to provide secure dynamic routing in WSN.Dynamic routing uses a dynamic routing protocol to automatically select the best route to put into the routing table. So instead of manually entering static routes in the routing table, dynamic routing automatically receives routing updates, and dynamically decides which routes are best to go into the routing table. It's this intelligent and hands-off approach that makes dynamic routing so useful.

Dynamic routing protocols vary in many ways and this is reflected in the various administrative distances assigned to routes learned from dynamic routing. These variations take into account differences in reliability, speed of convergence, and other similar factors .
OSPF defines the following router types:

- Area border router (ABR)
- Autonomous system boundary router (ASBR)
- Internal router (IR)
- Backbone router (BR)

The router type is an attribute of an OSPF process. A given physical router may have one or more OSPF processes. For example, a router that is connected to more than one area, and which receives routes from a BGP process connected to another AS, is both an area border router and an autonomous system boundary router.

### *3.2 Links-State Packets*

Link State Packet is a packet of information generated by a network router in a link state routing protocol that lists the router's neighbors. There are different types of Link State Packets, those are what you normally see in an OSPF database. Router Link, Summary Link, Network Link, External Link. Area Border Routers (ABRs) is a router that connects one or more OSPF areas. It is considered a member of all areas it is connected to. An ABR keeps multiple copies of the link-state database in memory, one for each area to which that router is connected. Below is a configuration for an ABR. Network statements describe which interfaces we should include in OSPF LSA(Link-state advertisement), and to which areas they correspond.
OSPF uses link state packets (LSPs) which are special datagram's that determine the names of and the cost or distance to any neighboring routers and associated networks

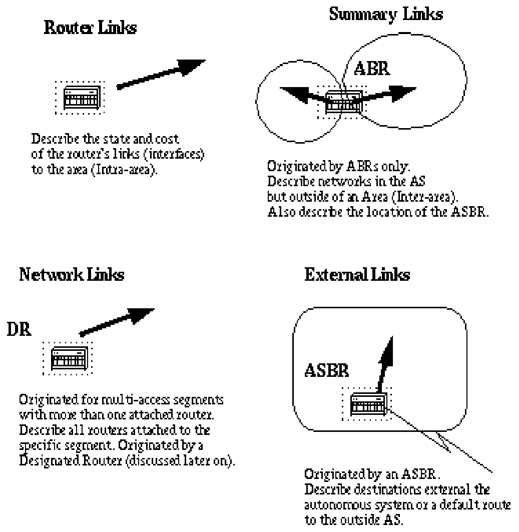
Router Links
Describe the state and cost of the router's links (interfaces) to the area (Intra-area).
Summary Links
ABR
Originated by ABRs only. Describe networks in the AS but outside of an Area (Inter-area). Also describe the location of the ASBR.
Network Links
DR
Originated for multi-access segments with more than one attached router. Describe all routers attached to the specific segment. Originated by a Designated Router (discussed later on).
External Links
ASBR
Originated by an ASBR. Describe destinations external the autonomous system or a default route to the outside AS.

Fig.2: Link-State Packets Diagram [12][1].

### *Proposed System Architecture*

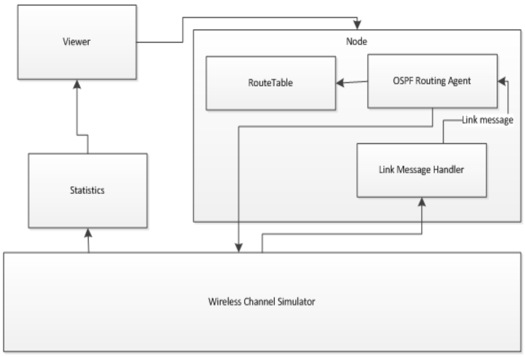

Fig.3: System Architecture [1]

The System architecture explains the overall functionality of the project. Complete functionality has been implemented in modules Node and Secure_efficient_routing. User can configure the number of nodes, position of nodes in the network and the communicate range of the nodes. User also views the routing table at any node.
**Node** : This module implements the functionality of wireless sensor node. Node need to know the routing path to another node. The routes are maintained in the routing table. To learn the route, Node uses the OSPF routing agent, which sends link messages to nearby neighbors. Form the link state messages the routing path are learnt dynamically.
**Secure_Efficient_routing** : This module is the core of the routing which learns the routing using the link state message and build a shortest path route to each other node and loads it to the routing table. The Functionality of this module is to do secure efficient dynamic routing. Shortest Routing path is calculated according to the Dijktra's algorithm. The user can view the node position & location which are placed randomly through this module.
When Node wants to send data to any other Node it will use the Routing table to get the route and send packet in that route. The Routing table gets updated dynamically in this module. The performance analysis done by collecting the parameters such as packet delivery ratio, Number of Nodes, Routing cost.
OSPF Routing Agent
OSPF Routing Agent implements the OSPF Routing. Each node requires complete topology information. Link state information must be flooded to all nodes
The working of OSPF in terms of steps is given below.
1. Each node establishes a relationship ("adjacency") with its neighbors
2. Each node uses its link state database to run a shortest path algorithm (Dijkstra's algorithm) to produce the shortest path to each network.

### OSPF Vs AODV

OSPF is a proactive link-state protocol for routing within autonomous systems. Sensor systems are by necessity autonomous; we wish to explore the applicability of this wire line protocol in the realm of sensor networks. The idea is to make OSPF aware of the sensor constraints, while maintaining its original features that made it attractive originally, viz. careful database synchronization and reliable flooding.

AODV is a reactive routing protocol for mobile ad hoc networks. It is its configuration parameters (i.e. soft state refresh intervals) that address node mobility. That is, the protocol should converge to steady state in zero mobility use cases. Performance Parameters are compared by taking Proposed OSPF Vs AODV.

For Implementation of the proposed system Dijkstra's Algorithm is used to find the shortest path between the nodes.

### *3.3 DES Algorithm*

This is algorithm used for providing security for the messages so that no one can modify the messages sent from source to destination.

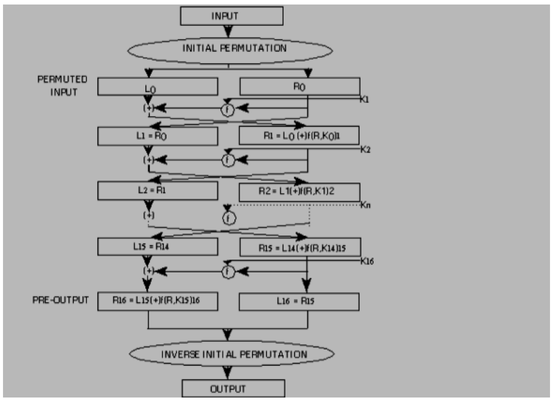

Fig 4 DES Algorithm

***Flowchart of the Proposed System***

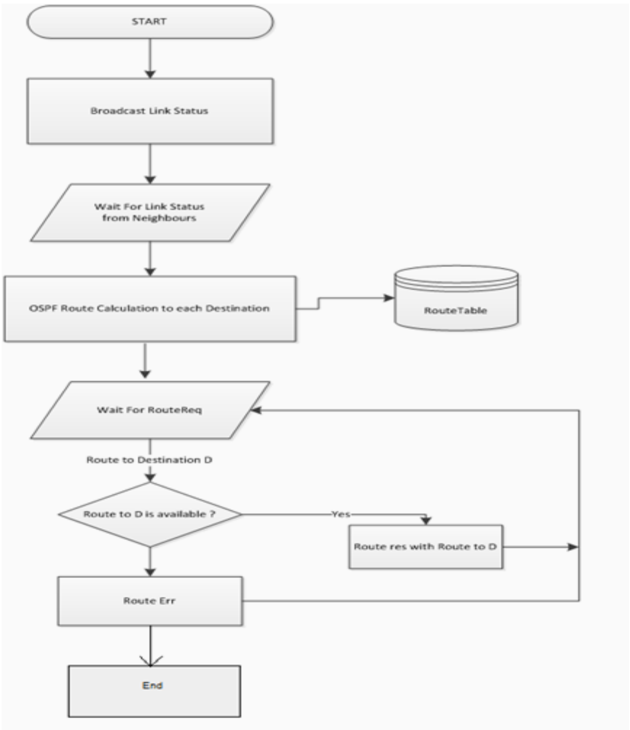
START
Broadcast Link Status
Wait For Link Status from Neighbours
OSPF Route Calculation to each Destination
RouteTable
Wait For RouteReq
Route to Destination D
Route to D is available ?
Yes
Route res with Route to D
Route Err
End

Fig 5   Flowchart of the system [1].

## IV.   ADVANTAGES

Dynamic routing uses a dynamic routing protocol to automatically select the best route to put into the routing table. So instead of manually entering static routes in the routing table, dynamic routing automatically receives routing updates, and dynamically decides which routes are best to go into the routing table. Its this intelligent and hands-off approach that makes dynamic routing so useful. Dynamic routing protocols vary in many ways and this is reflected in the various administrative distances assigned to routes learned from dynamic routing. These variations take into account differences in reliability, speed of convergence, and other similar factors

## V. RESULTS

The Simulation of Secure Efficient Dynamic Routing in Wireless sensor network has been implemented. Using Algorithm dijkstra's shortest path has been calculated. For providing security to the messages DES algorithm is used. The messages are encrypted and decrypted using this algorithm in order to provide security. User can be able to create number of nodes in the network. User can be able to send the packets using shortest path so that it reaches fast. User can also able to view the Routing Table at each node. User can also be able to view different nodes placed with their Node location and Node id. Performance Analysis done by comparing proposed Vs AODV protocol. For Doing Performance Analysis jfree chart is used.

## VI. PERFORMANCE ANALYSIS

The performance Analysis Parameters are Delivery Ratio, Routing Overhead in OSPF over RIP. From the results it proved that the Ospf Dynamic Routing in Wireless sensor networks is having Advantages over AODV in Sensor Networks.

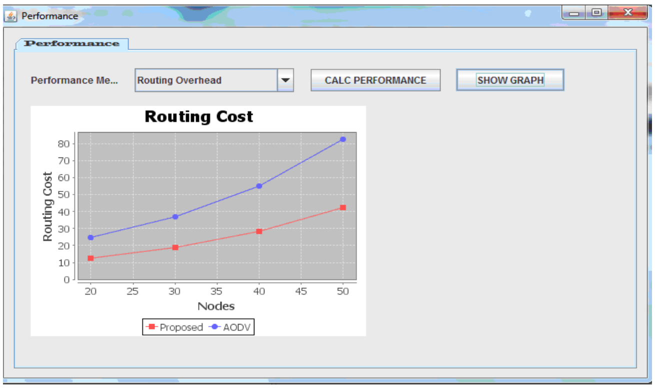
Performance Me... Routing Overhead

Fig.6 Routing Overhead

Fig .4 shows the comparison for proposed & AODV by taking performance parameter Routing Overhead. Performance Analysis has been done for 20 to 50 nodes.. Since The Routing cost is very less as compared to other protocol. It can be conclude that OSPF is better than AODV

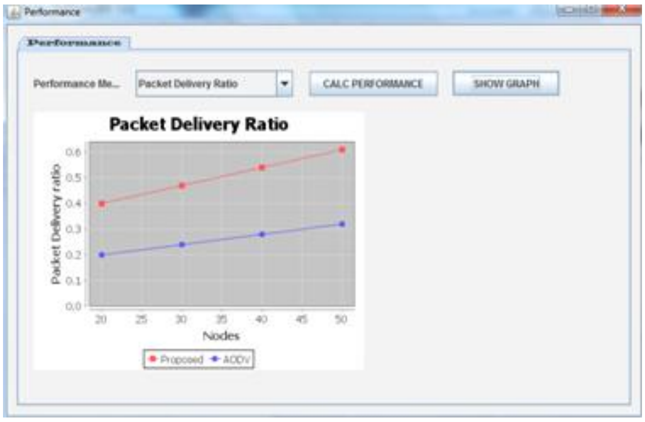
Performance Me... Packet Delivery Ratio

Fig.7 Packet Delivery Ratio

*Published By:*
*Blue Eyes Intelligence Engineering*
*and Sciences Publication (BEIESP)*

Fig .5 shows the comparison for proposed & AODV by taking performance parameter Packet Delivery Ratio. Performance has been analysis done for 20 to 50 nodes. Since it sends more packets as compared to other protocol. It can be conclude that OSPF is better than AODV.

## VII. CONCLUSION

From the Implementation it can be conclude that the proposed technique is very cost effective, secure and simpler to configure. From the performance Analysis it is clear that OSPF Routing in Wireless Sensor Networks is Very cost effective and more number of packets can be sent. Messages are secure because of using DES Algorithm.

## VIII. FUTURE ENHANCEMENTS

The future scope of this project can further enhanced for Node Level Security and also Energy consumed at each level can be displayed. This project can also be implemented such that it can be applicable to real world for wireless sensor network devices. It can also be extended to for the implementation of AES cryptography to increase the security. Hence saves from malicious, vulnerable intrusion attacks and is effective in protecting against denial of service and battery attacks.

## REFERENCES

[1]. Shobha.K P.G Student, Mamtha Jadhav.V Assistant Professor, Develop and Simulate a Secure Efficient Dynamic Routing Using Protocol in Wireless Sensor Network ISSN: 2277-3754 ISO 9001:2008 Certified International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012.

[2] Namarta Kapoor, Nitin Bhatia, Sangeet Kumar, Simranjeet Kaur Wireless Sensor Networks: A Profound Technology International Journal of Computer Science and technology - IJCST Vol. 2, Issue 2, June 2011.

[3] Kurt Stammberger, Mocana, Security in Wireless Sensor Networks An RTC Group Publication WIRELESS NETWORKS The magazine of record for the embedded computing industry July 2009.

[4] P. S. Pandian, K. P. Safeer, Wireless Sensor Network for Wearable Physiological Monitoring JOURNAL OF NETWORKS, VOL .3, No.5, May 2008.

[5] ZHAO Lei1, ZHANG Wei-Hong, XU Chao-Nong, XU Yong-Jun, LI Xiao-Wei1. Energy-aware System Design for Wireless Sensor Network Vol. 32, No. 6 ACTA AUTOMATICA SINICA November, 2006.

[6] Chris Karlof, David Wagner, Secure routing in Wireless Sensor Networks: Attacks and Countermeasures University of California at Berkeley.

[7] Chinese Journal of Electronics Vol.21, No.2, Apr. 2012 DRMA: A Dynamically Reconfigurable Management Architecture for Wireless Sensor Networks.

[8] Computer Networks by Patterson.

[9] Kurt Stammberger and Monique Semp, Introduction to Security for Smart Object Networks Internet Protocol for Smart Objects (IPSO) Alliance February 2010.

[10] Industry Insight -Security for Wireless Networks Security in Wireless Sensor Networks. July 2009.

[11] Sen,Jaydip ,Routing Security Issues in Wireless :Attacks and Defenses Author Networks 2011.

[12] Ospf Design Guide document id: 7039.

[13] Ronghui Hou, Member, IEEE, King-Shan Lui, Senior Member, IEEE, Fred Baker, and Jiandong Li, Senior Member, IEEE Hop-by-Hop Routing in Wireless Mesh Networks with Bandwidth .IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 11, NO. 2, FEBRUARY 2012.

[14] Jie Yang, Student Member, IEEE, Yingying Chen, Senior Member, IEEE,Wade Trappe, Member, IEEE, and Jerry Cheng, Detection and Localization of Multiple Spoofing Attackers in wireless sensor network.

[15] Yogendra Kumar Jain, Vismay Jain An Efficient Key Management Scheme for Wireless Network, International Journal of Scientific & Engineering Research, Volume 2,Issue 2, February-2011.