Secure Load-Balancing Routing for service-oriented WSN

Mr. Adhikrao.Y.Jadhav

System Admin , A.D.C.E.T, Ashta,Sangli.
416301-India.

Dr. Shivaji D. Mundhe,

Director -MCA –SIMCA
Sinhgad Institute of Management and Computer Application
Email:director_mca_simca@sinhgad.edu,
drshivaji.mundhe@gmail.com:

Miss.Tejashree Vishnu Khude

M.E. (CSE),AMGOI,Vathar

Prof.Dr.D.S.Bhosale

AMGOI,Vathar

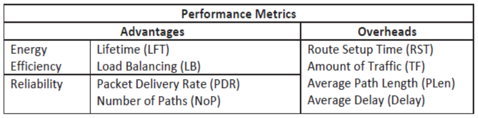
ABSTRACT--Wireless sensor networks (WSNs) comprise of motes interacting with the physical environment and collaborate among each other to provide data to the end-users. A Secure Routing capabilities on the order of Node to Base Station will be capable of both wired connectivity to the internet as well as wireless connectivity to the sensor network.

Service-oriented architectures for wireless sensor networks (WSNs) have been proposed to provide an integrated platform, where new applications can be rapidly developed through flexible service composition. In WSNs, the existing multipath routing schemes have demonstrated the effectiveness of traffic distribution over multipaths to fulfill the quality of service requirements of applications. However, the failure of links might significantly affect the transmission performance, scalability, reliability, and security of WSNs. Thus, by considering the reliability, congestion control, and security for multipath, it is desirable to design a reliable and service-driven routing scheme to provide efficient and failure-tolerant routing scheme. evaluation metric, path vacant ratio, is proposed to evaluate and then find a set of link-disjoint paths from all available paths. A congestion control and load-balancing algorithm that can adaptively adjust the load over multipaths is proposed. A threshold sharing algorithm is applied to split the packets into multiple segments that will be delivered via multipaths to the destination depending on the path vacant ratio. Simulations demonstrate the performance of the adaptive and secure load-balance routing scheme.

1. INTRODUCTION

Advantages in communication technology allow us to build the networks where large numbers of low-power and inexpensive sensor devices are integrated in the physical environment and operating together over a wireless media. In wireless sensor networks, sensor device, also may be referred as sensor node or node, perhaps is the most widely used equipment. Because these protocols have not been designed with security as a goal, it is unsurprising they are all insecure.

The service-oriented WSN aims at combining scalable wireless sensing technology with independent service provisioning, where the applications are treated as services that can support via more flexible protocol design and resource management. Both generic and application-specific WSNs would benefit from service-oriented architecture and avoid most of their limitations. In service-oriented applications, services with various performance metrics, e.g., bandwidth, delay, load balancing, and reliability, have been well studied within the service systems.



Performance Metrics		
Advantages		Overheads
Energy Efficiency	Lifetime (LFT) Load Balancing (LB)	Route Setup Time (RST) Amount of Traffic (TF) Average Path Length (PLen) Average Delay (Delay)
Reliability	Packet Delivery Rate (PDR) Number of Paths (NoP)	

Table 1. Performance Matrics

Where each node provides the quality-of-service (QoS) parameters associated with these services. In a service-oriented WSN, applications can be designed over service requirements to depart from current application-specific or generic WSNs [4]. A large volume of traffic is exchanged over WSNs; as a result, how to improve the throughput of WSNs is a critical challenge in the design of service-oriented WSNs. It is desirable to design an adaptive multipath

Routing scheme that is able to significantly reduce the downstream traffic and dynamically support QoS requirements, as well as achieve reliable paths from a source node to a destination node. Each node on a path should be able to evaluate the performance of its next-hop neighbors according to the reliability of the path. The multipath routing scheme should be able to provide the services with bandwidth guaranteed multipaths, which help these services be run over secure and reliable network architecture.

2. Routing taxonomy in WSNs

Routing protocols in wireless sensor networks can be classified into following categories

2.1 According to Deployment:

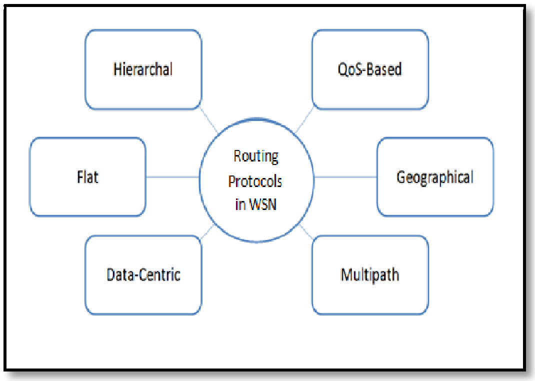


Figure 1. Routing Protocols

- Data-Centric: Routing, usually sink ask for specific node data by broadcasting a message. After this message is reached to the specific node which sink is interested in its data, it will send the information back to sink.
- Flat: Routing uses tremendous equal sensor nodes (in case of memory, processor and so on) which collaborate together in order to sense the environment.
- QoS-Based: Routing is performed by applying QoS parameters which usually control packet overhead and energy efficiency
- Geographic: Routing uses location information of the node to forward data. By applying this approach, overhead may significantly decreases.
- Multipath: Multiple paths from source to destination are created and packets will send to destination through these paths.
- Hierarchal routing: Routing (also called as cluster-based routing), the virtual tree is made by the nodes. Each node sends the packet to base (root of the tree) through the parent node.

2.2 Types of Routing Techniques

A. Single path routing technique

it is easy for the source node to select the inter-mediate data routing nodes from the same part of the network over and over again. In single path routing, the presence of a malicious node on the path can manipulate and corrupt the data without catching the attention of the sink node.

B. Multipath routing technique

Multipath routing is an alternative routing technique, which selects multiple paths to deliver data from source to destinationMultipath routing is an efficient technique to route data in wireless sensor networks (WSNs) because it can provide reliability, security and load balance, which are especially critical in the resource constrained system such as WSNs. In this paper we provide a survey of the state-of-the-art of proposed multipath routing protocols for WSNs, which are classified into three categories, infrastructure based, non-infrastructure based and coding based, based on the special techniques used in building multiple paths and delivering sensing data.

2.3 Routing Schemes categories

Each node over these links should be able to sense, process, and transmit information of the monitored area, in which the routing scheme is one of the most critical design issues in WSNs and a huge number of routing schemes have been proposed. Most of these routing schemes can be classified into four categories:

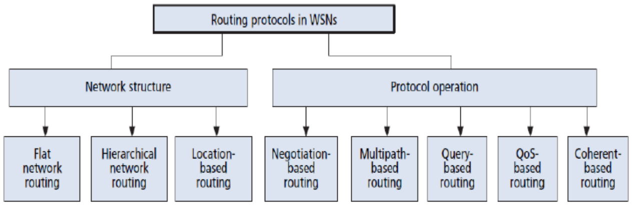


Figure 2. Routing protocol schemes

- Multipath-based routing scheme

The multipath routing scheme should be able to balance load and provide high aggregate bandwidth and fault tolerance on multipaths.

- query-based routing scheme
  Query-based routing protocols start to work as the destination (sink) asks for the data and then corresponding nodes will forward data to the destination.
- negotiation-based routing scheme
  Query-based routing protocols start to work as the destination (sink) asks for the data and then corresponding nodes will forward data to the destination.
- QoS-based routing scheme.
  Try to satisfy QoS metrics such as bandwidth or delay and make a balance between energy consumption and data quality as well

3. CLASSIFICATION OF EXISTING MULTIPATH ROUTING TECHNIQUES

3.1 Existing multipath routing techniques

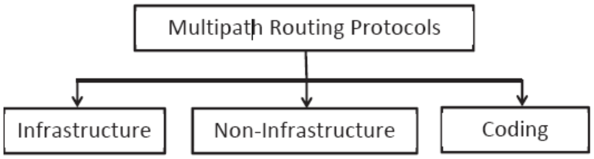


Figure 3. Multipath Routing protocols

3.1.1 Infrastructure Based Multipath Routing Protocol

The most important features of the infrastructure based multipath routing protocol is the construction and maintenance of multiple paths from source to destination. Any specific topology structure can help to build an efficient route from source to destination. For example, in a spanning tree.On the basis of heuristic information such as node's location, position in the structure and capability, multiple paths are discovered. These discovered paths are usually node-disjoint paths, which help to avoid data collision and interference. An infrastructure provides reliable and fast data transmission because every intermediate data routing node has its next hop set up in advance.

3.1.2 Non-Infrastructure Based Multipath Routing Protocols

Protocols which do not construct any infrastructure in order to transmit the data are considered non-infrastructure multipath routing protocols. The major difference between infrastructure based routing protocol and non-infrastructure based routing protocol is as follows. The path is discovered prior to the data transmission in infrastructure based routing protocol.

3.1.3 Coding Based Multipath Routing Protocols

This category consists of multipath routing protocols that use coding tech- unique in data transmission. In infrastructure based protocols, path construction and maintenance are two major overheads. Data transmission, however, will be straight forward by following the established routes, although in order to achieve reliability the same data packet is transferred through all multiple paths. This is energy inefficient and not secure. On the contrary, the non- infrastructure based protocols have no path construction and maintenance overheads, but have problems with secure data transmission and less likelihood of successful delivery on the sufficient number of paths. Therefore both the above categories have two common problems, unnecessary redundancy in transmission and security.

3.2 Drawbacks in existing schemes:

3.2.1 The infrastructure based protocols-

Path construction and maintenance are two major overheads. Data transmission, however, will be straight forward by following the established routes, although in order to achieve reliability the same data packet is transferred through all multiple path. This is energy inefficient and not secure.

3.2.2 The non-infrastructure based protocols –

Have no path construction and maintenance overheads, but have problems with secure data transmission and less likelihood of successful delivery on the sufficient number of paths.

3.2.3 The coding based –

Simultaneous transmission of data from node disjoint paths may cause high data packet loss and affects the transmission performance. On the other hand, failure in the consecutive nodes due to several obstacle can decrease the effectiveness of the coding scheme.

4. WHY WE USE MULTIPATH ROUTING SCHEMES ?

4.1 To overcome this challenge design an adaptive multipath routing Scheme

5. Reduce the downstream traffic
6. Dynamically support qos requirements provide

3. The services with bandwidth guaranteed multipaths
4. Services be run over secure and reliable network architecture.
5. Link-disjoint-based multipath routing is a good idea to treat each application as a service task.

4.2 Advantages of Multipath Routing

- ❑ Data Reliability

  Data Reliability can be defined as the ratio of the amount of data received by the destination node to the amount of data sent by the source node.
- ❑ Data Security

  Multipath routing can improve security because of the nature of multiple paths
- ❑ Energy-Efficient

  Efficient use of energy is necessary to maximize the network lifetime.
- ❑ Load distribution

  Load distribution using multipath routing helps to improve the network lifetime by delaying the appearance of network partition

5.CHALLENGES IN BUILDING MULTIPATH ROUTING PROTOCOLS

6.

<u>5.1 The design of multipath routing protocol. These questions answers to these questions are like follows.</u>

In multipath routing, multiple paths are discovered to distribute the network traffic and prolong network lifetime; however, there are several major questions to be addressed in the design of multipath routing protocol. These questions are like follows.

1. How many paths are optimal?
2. How does one discover those optimal paths?
3. How does one maintain discovered paths and distribute the data among those paths? Many algorithms utilizing intelligent techniques and different design principles have been proposed in the search for answers to these questions.

5.1.1 Number of Routes.

In multipath routing, reliability and security are functions of the number of paths selected for transferring data from source to destination. If there is not a su_cient number of paths available between source and destination, achieving the goal of multipath routing is not possible.

5.1.2 Route Discovery.

The nodes in the WSN act as data sender as well as data router. Once the data packet has arrived at an intermediate routing node, it must select the next node having the capability of passing the data packet in the direction of the sink.

5.1.3 Consumption of Resources.

In WSN the efficient resource consumption at each node is necessary in order to increase the network lifetime. In multi-path routing many messages are exchanged among nodes in order to discover the optimal paths between source and destination.

5.1.4 Path Maintenance.

In multipath routing, the usage of multiple paths from source to destination needs to be maintained periodically in order to achieve high data reliability as well as load balance among multiple paths.

6.SECURE AND ADAPTIVE LOAD-BALANCING MULTIPATH ROUTING SCHEME

<u>6.1 service-oriented multipath AODV (shortly as SM-AODV), which includes the following features.</u>

6.1.1) By considering the security of data delivery, we propose a novel technique for data delivery via multipaths. It is the first phase of our adaptive load-balancing multipath

Routing scheme to enhance the data confidentiality in the service-oriented WSNs, which is similar to secure protocol for reliable data delivery.

6.1.2) A load-balancing approach that computes the path vacant ratio of multipaths is proposed for multipaths. The path vacant ratio can be used to evaluate the load over multipaths, which is derived from taking account of load balancing, path load, important paths, and importance of nodes over multipaths. .

6.1.3) An adaptive congestion control scheme is proposed to adaptively adjust packet delivery rate over each path according to the congestion level that maintained the HELLO message. Each intermediate node on active paths is able to adaptively detect the occurrence of congestion and then notify the parent nodes to reduce the packet delivery rate according to the congestion level. Each node monitors its traffic load; when congestion occurs, it will update the congestion information in the HELLO message and then send the message to its parent nodes.

<u>6.2 Load-Balancing Multipath Routing Scheme</u>

6.2.1 The evaluation of multipath contains five steps as given in the following example

- **STEP 1** -At first, take the following assumptions:

1) the network is a static wireless network
2) node S is the source and D is the destination
3) all nodes are working on the same radio and channel.

- **STEP 2- It can be seen from fig.1**

1) Path1: L1 SD = {S, a, b, c,D}
2) Path2: L1 SD = {S, a, d, c,D}
3) Path3: L1 SD = {S, a, d, e,D}
4) Path4:L1 SD = {S, f, d, c,D}
5) Path5: L1 SD = {S, f, d, e,D}
6) Path6: L1 SD = {S, f, g, e,D}.

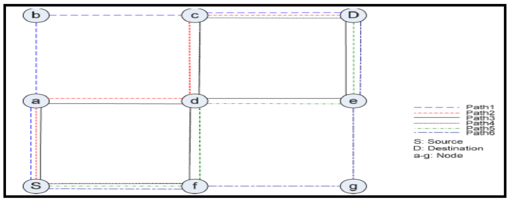


Fig. 4 six paths from S to D:

STEP 3- According to the connectivity graph, the adjacent matrix **A** can be derived as follows:

$$A = \begin{array}{c|ccccccccc} & S & a & b & c & d & e & f & g & D \\ \hline S & 0 & 0 & 0 & 3 & 0 & 0 & 3 & 0 & 0 \\ a & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ b & 0 & 1 & 0 & 0 & 2 & 0 & 0 & 0 & 3 \\ c & 3 & 1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ d & 0 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 0 \\ e & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 2 \\ f & 3 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 0 \\ g & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ D & 0 & 0 & 3 & 0 & 0 & 2 & 0 & 0 & 0 \end{array}$$

STEP 4-Then, the connectivity degree of each node can be calculated by

$$C(n_i) = \sum_{k=0}^{N+1} a_{ik}$$

and we have $C(S) = 6$, $C(a) = 2$, $C(b) = 6$, $C(c) = 6$,$C(d) = 8$, $C(e) = 5$, $C(f) = 6$, $C(g) =2$, and $C(D) = 5$.

STEP 5- For each path, we can calculate the path importance degree according to the connectivity degree of each intermediate node on it

$$PI(\text{path}_i) = \sum_{j=S}^{D} C_{n_j}$$

The weight of each path can be obtained according to as

$$w_i = \frac{PI(\text{path}_i)}{\sum_{i=1}^{N} PI(\text{path}_i)}$$

$W = \{wi,\ 1 \le i \le 6\} = \{14.46\%,\ 17.47\%, 18.07\%,\ 18.07\%,\ 17.47\%,\ 14.46\%\}$, and the

Vacancy rate of each path can be obtained according to

$$v_i = \frac{\sum_{i=1}^{N} PI(\text{path}_i) - PI(\text{path}_i)}{\sum_{i=1}^{N} PI(\text{path}_i)}.$$

as $V = \{vi,\ 1 \le i \le 6\} = \{17.11\%,\ 16.51\%,\ 16.38\%,\ 16.38\%,\ 16.51\%,\ 17.11\%\}$,
Which is the criterion for delivering of packets over multipaths.

6.2.2 CONGESTION CONTROL SCHEME FOR MULTIPATH

Multipath discovery and maintenance involve finding the multiple paths between a source node and a destination node. A set of link-disjoint paths can be easily found by the method

A. Congestion Detection

Congestion detection is a technique to detect congestion based on buffer occupancy as well as the wireless channel load. The congestion control scheme for multipaths includes the following three main stages: 1) congestion detection; 2) congestion control and notification; and 3) congestion cancellation and load adjustment. Here, an efficient congestion control scheme will be proposed, which is able to adaptively schedule the load distributive to multiple paths and reduce the congestion on multipaths to avoid packet loss and thus enhance the throughput, security, and reliability of traffic.

Algorithm 1 Congestion Detection Algorithm

```
Input: pk(m)
Output: Adjust rate according to CONGEST
CongestDetection();
for m ← 1 to M do
    special treatment of the first element of line i;
    if 0.95 ≤ pk(m) then
        SetCongestLevel(CONGEST_LEVEL,0);
    else if 0.75 ≤ pk(m) ≤ 0.95 then
        SetCongestLevel(CONGEST_LEVEL,1);
    else if 0.4 ≤ pk(m) ≤ 0.75 then
        SetCongestLevel(CONGEST_LEVEL,2);
    else
        SetCongestLevel(CONGEST_LEVEL,3);
    PacketCongest2Hello(); SendHelloMessage();
end
while (CheckCONGESTEvent()) do
    if fCongSentk == TRUE then
        switch(CONGEST_LEVEL)
        case 0: break;
        case 1: break;
        case 2: AdjustLoad();ResetEWM();break;
        case 3: AdjustRate();ResetEWM();break;
        default: break;
    end
end
```

B. Congestion Control and Notification for Multipath

We use a hop-by-hop rate adjustment mechanism to tune the congestion on multipaths, where the output rate at a node on a particular path m is controlled by adjusting a scheduling rate Risch. The scheduling rate is defined as how many packets are scheduled at a time interval from the priority queues on a particular path, as shown in Fig. 5

nodes of *ni* find that the packet service ratio of parent *nj* is lower or greater than a threshold, then the multipath rate control procedure will be triggered.

ISBN:978-93-5254-640-4

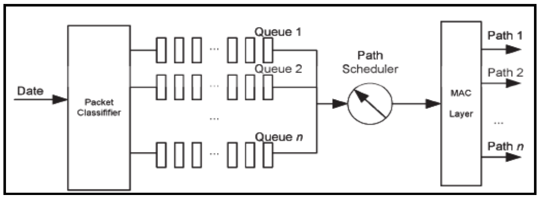


Fig. 5. Congestion path schedule.

C. Congestion Cancellation and Load Adjusting

The congestion cancellation procedure empties its buffer and reduces the amount of backlogged data packets to allow the current data packet to be transmitted before sending the CONGEST message to the source node. When a CONGEST packet is received by the source node, the delivery rate is adjusted to a lower predefined rate (such as one-half, one fourth, one-sixth, one-eighth, and so forth depending on the CONGEST_LEVEL)

Algorithm 2 Adjustment Algorithm
Input: Current rate
Output: Adjust delivery rate

```
Check the CONGEST message;
if (CheckForCongestion() && fConfigSend ==
FALSE)
then
PurgeOwnDataBuffer();
SendCONGPCKTOSOURCE();
ResetEWMAvg();
end
for m ← 1 to M do
switch(CONGEST_LEVEL){
case RATE_LEVEL_0:
currentRate = RATE_LEVEL_0;break;
case RATE_LEVEL_1:
currentRate = RATE_LEVEL_1;break;
case RATE_LEVEL_2:
currentRate = RATE_LEVEL_2;break;
case RATE_LEVEL_3:
currentRate = RATE_LEVEL_3;break;
PacketCongest2Hello();
SendHelloMessage();
}
End
```

6.2.3 SECURE MULTIPATH LOAD-BALANCING ROUTIN SCHEME IN WSN

In order to provide more secure protection for the multipath routing approach, this work exploits a threshold secret sharing method to split the data into a number of shares. For SM-AODV, we first apply a threshold secret sharing method to split the data into a number of shares which will be packed into more data packets that will be delivered to multipaths according to load on each path as mentioned previously. If the load on one path increases, SM-AODV can decrease the number of packets to that path according to the path vacant rate.

SM-AODV includes three phases:

1. **packet delivery**

   Use the threshold secret sharing algorithm to split the data into multiple segments.

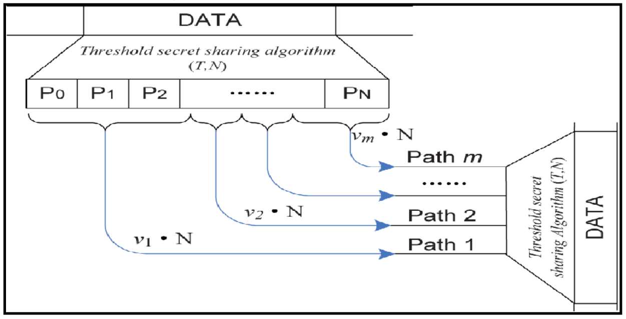


Figure 5. Packet delivery scheme

2. **multipath evaluation and scheduling**
   1) SM-AODV finds nondisjoint paths which can be more easily discovered. After this step, all nondisjoint paths from the source to the destination can be obtained, as shown in Fig. 4.
   2) Multipath load-balancing evaluation. The multipaths are evaluated according to the procedure mentioned previously, and the output of this phase is the path vacant rate of each path.
   3) As described in phase one, we need to split the load according to the threshold secret sharing algorithm.
   4) Deliver the distributed load to multipaths according to the path vacant rate.
   5) Set up the congestion control module to monitor the CONGEST events. If CONGEST events arrive, then invoke the congestion control mechanism and schedule the load according to the CONGEST_LEVEL.

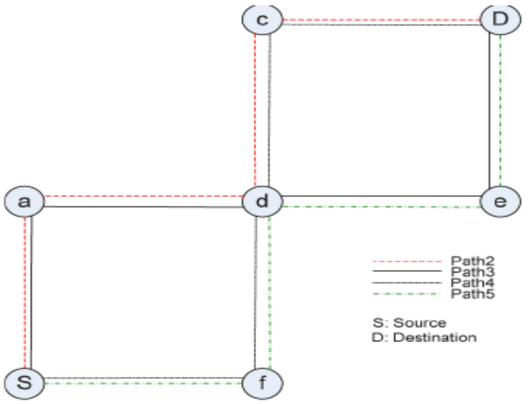


Fig. 4. Congestion networks, in which congestion may be caused by feasible paths at node *d*

3. Congestion Control

In this phase, each node monitors the CONGEST event by checking the HELLO message from child nodes.

Congestion cancellation and load adjustingthe rules of adjustment are as follows.

1) CONGEST_LEVEL = 0: The nodes do not do anything. It means that the path is not congested and every path is on the best status.

2) CONGEST_LEVEL = 1: It means that the load is normal and each path is working well.

3) CONGEST_LEVEL = 2: It means that the paths are congested on the node. It has to adjust the load by reducing the sending rate to the next lower rate.

4) CONGEST_LEVEL = 3: It means that the paths are congested heavily and the multipaths must be updated. This situation may occur when intermediate nodes fail or suffer from power off

7. CONCLUSION

1. Introduced an adaptive load-balancing multipath routing protocol (SM-AODV) for WSNs that uses load balancing, congestion control, and secure delivery scheme to address the limitations in existing multipath routing schemes.
2. Additionally reviewed some of concepts and issues concerns with security in multipath.
3. In SM-AODV, the packets are delivered across multipath using a secure and reliable scheme, which decouples the node's capabilities for applications and offers optimization alternatives not available in current schemes yet..
4. This scheme provide effective routing performance for multipath and enable WSNs to provide reliable application-level services.

REFERENCES

Papers

1. Empirical Study on Secure Routing Protocols in Wireless Sensor Networks
2. IEEE SYSTEMS JOURNAL, VOL. 8, NO. 3, SEPTEMBER 2014

Adaptive and Secure Load-Balancing Routing Protocol for Service-Oriented Wireless Sensor Networks. Shancang Li, *Member, IEEE*, Shanshan Zhao, Xinheng Wang, *Member, IEEE*, Kewang Zhang, and Ling Li

3. Multipath Routing Techniques In Wireless Sensor Networks: A Survey Kewei Sha, Jegnesh Gehlot and Robert

4. International Journal of Wireless & Mobile Networks (IJWMN) Vol.2, No.4, November 2010

DOI : 10.5121/ijwmn.2010.2402 13

PERFORMANCE COMPARISON OF LINK, NODE AND ZONE DISJOINT MULTI-PATH ROUTING STRATEGIES AND MINIMUM HOP SINGLE PATH ROUTING FOR MOBILE AD HOC NETWORKS

Links

www.IJCSI.org
www.IEEE.com
www.scholargoogle.co.in
www.sentilla.com