# Robust and Secure Load-Balancing Multipath Routing Protocol for Service-Oriented WSNs

[1]Shwetha K.N, [2]Ms. Sheela Sridhar
[1]M-Tech (2nd Year), [2]Associate Professor
[1]Department of Computer Science,
[1]BNM Institute of Technology, Bengaluru, India

***Abstract* - Service-oriented architectures have been proposed for wireless sensor networks (WSNs) in order to provide an integrated platform. New applications can be easily developed through services provided by them. Existing multipath routing protocols have demonstrated the distribution of traffic over multiple paths to fulfil the quality of service requirements of applications. However, link failure problem significantly affects the transmission performance, reliability, scalability and security of WSNs. Thus, it is very important to design a service-oriented routing scheme considering reliability, congestion control and security for multipath in WSNs. An evaluation metric, path vacant ratio is proposed in order to balance the load over multipath. A congestion control scheme that can adaptively adjust the load is proposed. A threshold secret sharing algorithm is applied to split the packet into number of segments that can be transmitted to the destination over multipath according to the path vacant ratio. The performance of SM-AODV is demonstrated using NS-2 simulator.**

***Index Terms* – Wireless sensor networks (WSNs), service-oriented architecture, multipath, load balance, congestion control.**

## I. INTRODUCTION

A wireless sensor network contains spatially distributed autonomous sensors that monitor physical or environmental conditions, such as sound, pressure, temperature etc. and pass their data through the network to a desired destination or location. A WSN is composed of dozens to thousands of devices, which are of low cost and reduced size, and are able to sense the data and transmit it through wireless connections. Sensors are constrained in terms of storage, energy and processing resources. They work together, extracting environmental data and transmitting them to user applications. Since sensors have predetermined battery power and usually have to operate for long periods of time, energy consumption is a major issue in WSNs. Since data transmission consumes largest source of energy, the communication protocols for WSNs come up with the solutions to minimize the number and range of transmissions, thus extending lifetime of the network. Most of the solutions presented by those protocols are based on short-range communication, multi hop and adopt some aggregation mechanism to decrease the amount of data transmission.

WSNs can be applied to a large range of applications with various requirements. Each application class has concrete needs and is best availed by a particular type of communication protocol. Thus, the cull of the most congruous protocol to each application class becomes a consequential issue. In general, it is arduous for application developers to cull the protocol that better meets their application needs. Therefore, a middleware is proposed for WSN that acts as a mediator between applications and the WSN and translates application requisites in an efficient cull of network configuration and protocols. The middleware is generic enough to be used over a sizably voluminous range of applications. The middleware adopts an accommodation approach, in which the WSN is optically discerned as an accommodation provider for utilizer applications. WSN provides services such as data accumulation and distribution. The primary services catered by middleware system are analysis of the application needs, best network protocol selection and configuration according to the needs. The middleware abstracts the generic WSN that provides services for various applications and also provides flexible way to access those services through high level languages. There are mainly two types of routing mechanisms, single path routing and multiple path routing. Single path routing is scalable and simple, but does not efficiently satisfy the requirements of resource restricted WSNs. Multipath routing is an effectual approach to route data in wireless sensor networks (WSNs) because it can provide security, reliability, and load balance, which are critical in the resource restricted WSNs. SM-AODV is a multipath routing protocol simulated in network simulator 2.

## II. LITERATURE SURVEY

In WSNs, the links between a source node and a destination node may be very weak and go down at any time. Each node over these links must be able to sense, process, and transmit data of the monitored area, in which the routing technique is one of the most challenging design issues in WSNs and a large number of routing schemes have been proposed. Most of these routing techniques can be classified into four categories: multipath-based routing scheme, query-based routing scheme, negotiation-based routing scheme, and QoS-based routing scheme. The multipath routing scheme must be able to balance load and provide high aggregate bandwidth and fault tolerance on multiple paths. Multipath routing protocols such as ad hoc on demand multipath distance vector

(AOMDV) [1], Temporally Ordered Routing Algorithm (TORA) [2], on-demand multiple route maintenance in AODV extensions (ORMAD) [3], and interference-minimized multipath routing (I2MR) [4] are the most common examples in ad hoc networks.

A. C. Valera et al., [1] have proposed a new routing protocol named CHAMP routing protocol for mobile ad hoc network. CHAMP employs collaborative packet caching and shortest multipath routing to reduce packet loss due to frequent route failures. AOMDV is an extension of ad hoc on-demand distance vector (AODV) that supports multipath by providing a number of loop-free and link-disjoint paths [1], where the control packet of AODV is redesigned and an advertising *hop-count* field and a *route-list* field that can deal with mobility-induced routing failures are added.

C. Li, J. Zou et al., [2] have studied a joint coding/routing optimization between network lifetime and video distortion by applying information theory to wireless visual sensor networks for correlated sources. TORA is an adaptive and distributed routing algorithm that provides multipath by building and maintaining a *directed acyclic graph* at a destination. In TORA, a local repair procedure will be invoked at the upstream node when links are broken.

Z. Yu and Y. Guan [3] have conducted an approach called ORMAD (On-demand Route maintenance in Multipath AODV) as a link-disjoint extension to TRAODV. This paper aims to ameliorate routing fault tolerance in mobile ad hoc networks by optimizing multipath routing in traditional AODV routing protocol.

T. Jenn-Yue et al., [4] have proposed path-set evaluation technique for multipath load balancing. In I2MR, the interference is minimized over multipath, and it supports the high-rate streaming. In fact, I2MR does not address the problem of robustness and security in its congestion control scheme, where the source node first delivers a packet on the main path and then delivers the next packet on the second path after two packet transmission intervals. Similarly, the source node repeats this process until all packets in the queue are transmitted. In the load-balancing scheme of I2MR, the packet loss on the primary or secondary path may cause long delays.

However, most existing multipath routing schemes suffer from the following four problems and developing an adaptive load-balancing protocol is still very challenging in WSNs.

1) A packet-distributing scheme at the source node results in routing security problems. For service-based applications, a secure packet-distributing scheme should be taken into consideration in the routing design.
2) Because of the susceptibleness of service-oriented WSNs, the load over the multipath must be balanced adaptively according to the rate on disjoint paths. In the multipath routing scheme, by distributing the workload to multiple paths, the lifespan of the WSN will be longer, and congestion can be reduced under heavy traffic.
3) In WSNs, congestion may decrease channel usage and cause the packet loss rate to rise that leads to packet drop and long packet delay. Congestion can be slightly decreased by general multipath schemes; however, it is still crucial to develop a more effective congestion control and rate adjustment scheme.
4) A multipath evaluation metric is still lacking. The quality of multipath is crucial for evaluation of load balancing and congestion control.

## III. PROPOSED SYSTEM

### A. Multipath load balancing routing scheme

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

### B. Secure multipath routing scheme

By considering the security of data distribution, a novel technique for data distribution via multipath is proposed. It is the first phase of adaptive load-balancing multipath routing scheme to enhance the data confidentiality in the service-oriented WSNs. The **secret sharing algorithm** is utilized to dissever the data packets according to the path vacant ratio. If the data are split into $N$ packets, the data can be perfectly recovered from any received $T$ out of $N$ packets. This is called a $(T,N)$ threshold secret sharing scheme in which $T$ is the threshold. With less than the threshold shares, one cannot recover any data of the sent packets. Fig. 1 shows packet delivery scheme in SM-AODV.

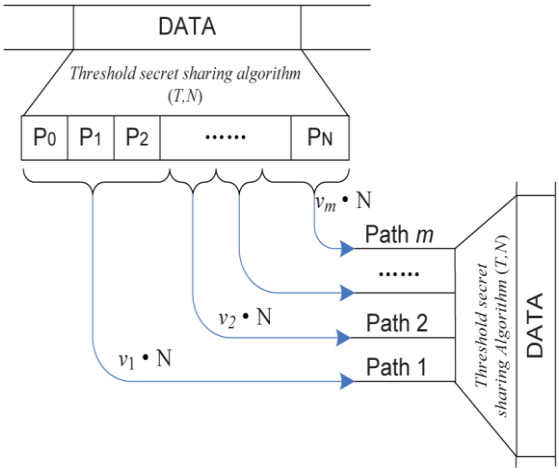


Fig. 1 Packet delivery scheme

### C. Congestion control scheme

An adaptive **congestion control scheme** is proposed to adaptively adjust packet distribution 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 distribution rate according to the congestion level. The congestion control technique for multipath contains the three main stages: 1) congestion detection; 2) congestion control and notification; and 3) congestion cancellation and load adjustment.

**Algorithm 1** Congestion Detection Algorithm

**Input:** *pk*(*m*)
**Output:** Adjust rate according to CONGEST

```
CongestDetection();
for m ← 1 to M do
        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(); break;
                case 3: AdjustLoad(); break;
                default: break;
        end
end
```

Congestion detection is a technique to detect congestion based on buffer occupancy and wireless channel load. The proposed congestion detection technique can provide service ratio and congestion notification when it occurs. Here, an efficient congestion control technique is proposed, which can adaptively schedule the load on multiple paths and reduce the congestion on multipath to avoid packet loss.

**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
```

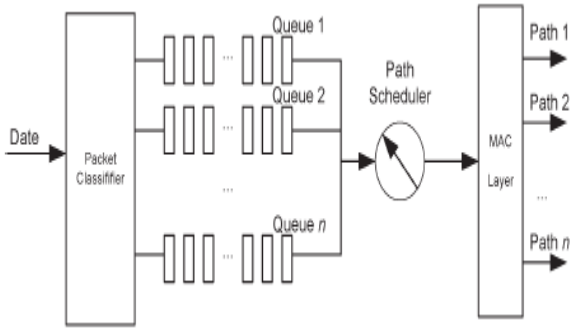


Fig. 2 Congestion path schedule

The congestion cancellation scheme 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 message is received by the source node, the packet 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). For some applications, when the load rate is too low or the source node receives multiple CONGEST packets that exceed the predefined limit from one route, it will call route rediscovery mechanism to find any other multipath. Fig. 2 shows scheduling congested path in SM-AODV.

## IV. RESULTS ANALYSIS

SM-AODV protocol is simulated using NS-2 simulator. Performance of SM-AODV is evaluated by comparing it with AOMDV in terms of throughput, packet delivery rate and end to end delay. Fig. 3 shows throughput, Fig. 4 shows packet delivery rate and fig. 5 shows end to end delay comparison of SM-AODV and AOMDV.

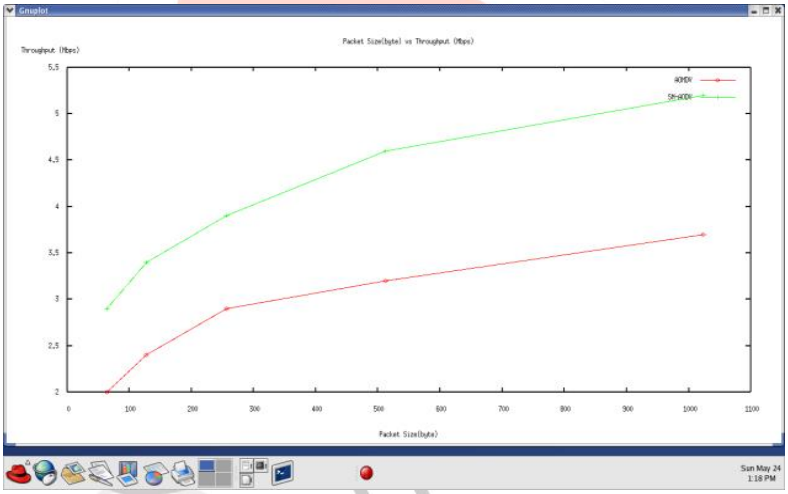


Fig. 3 Throughput

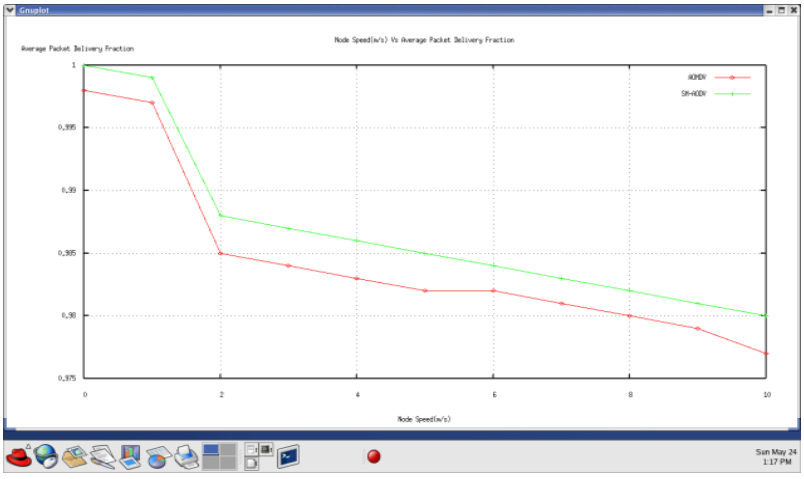


Fig. 4 Packet delivery rate

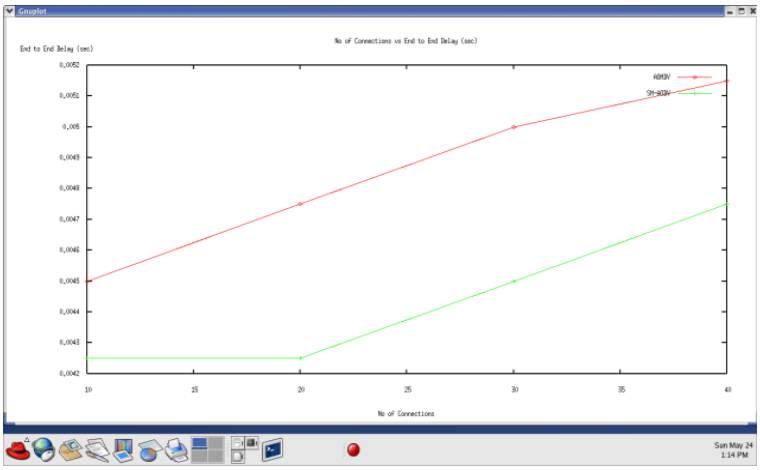


Fig. 5 end to end delay

## V. CONCLUSION AND FUTURE ENHANCEMENT

A Robust and secured load-balancing multipath routing protocol (SM-AODV) which includes secure delivery, load balancing, and congestion control scheme is developed in order to overcome the limitations of existing multipath routing techniques. In SM-AODV, the packets are sent across multiple paths using a secure and reliable technique, which differentiates the node's abilities for applications and recommends enhanced alternatives not present in current schemes yet. SM-AODV accomplishes significant reliability improvement in routing downstream traffic by using a secret sharing scheme at the source. SM-AODV uses an adaptive congestion control technique, which is effective even in the situation that node or link failure occurs regularly. SM-AODV increases packet delivery rate, throughput and decreases end to end delay.

When multiple paths are in use, packet reception order at the sink node may be different from the packet transmission order at the source node. This issue affects the performance of applications such as multimedia streaming and wastes network resources. Finally, the developments of multi-constrained QoS multipath routing protocols that guarantee the QoS demands of different applications are required. To achieve this, different multipath routing approaches should be integrated efficiently. Because of the dynamic behavior of SM-AODV protocol, it can be implemented by ad-hoc networks in future.

## VI. REFERENCES

[1] A. C. Valera, W. K. G. Seah, and S. V. Rao, "Improving protocol robustness in ad hoc networks through cooperative packet caching and shortest multipath routing," IEEE Trans. Mobile Comput., vol. 4, no. 5, pp. 443– 357, Sep./Oct. 2005.
[2] C. Li, J. Zou, H. Xiong, and C. Chen, "Joint coding/routing optimization for distributed video sources in wireless visual sensor networks," IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 2, pp. 141–155, Feb. 2011.
[3] Z. Yu and Y. Guan, "A dynamic en-route filtering scheme for data reporting in wireless sensor networks," IEEE/ACM Trans. Netw., vol. 18, no. 1, pp. 150–163, Feb. 2010.
[4] T. Jenn-Yue, H. Yajun, and T. Chen-Khong, "Interference-minimized multipath routing with congestion control in wireless sensor network for highrate streaming," IEEE Trans. Mobile Comput., vol. 7, no. 9, pp. 1124– 1137, Sep. 2008.
[5] J. Lu and T. Suda, "Differentiated surveillance for static and random mobile sensor networks," IEEE Trans. Wireless Commun., vol. 7, no. 11, pp. 4411–4423, Nov. 2008.