SERVICE-ORIENTED WIRELESS SENSOR NETWORKS WITH ADAPTIVE AND SECURE LOAD-BALANCING ROUTING PROTOCOL

Soumya M.G[1], Mrs. Manjula. G[2]
[1]M-Tech (2nd Year), Department Of Computer Network Engineering
[2]Asst. Prof., Department Of Information Science
East West Institution of Technology, Bangalore, India

Abstract: In Wireless Sensor Network, Service Oriented Architectures are proposed to provide an integrated platform, where new applications will be easily developed by the composition of services. The existing multipath routing schemes which we used in WSNs have demonstrated the effectiveness of distribution of traffic over the multipath to fulfill the requirements of applications. However, failure of links might affect the performance of the network and also the Scalability and reliability of WSNs. Thus, by considering the performance, scalability and reliability it is suitable to design a reliable and service-driven routing scheme to provide an efficient and failure-tolerant routing scheme. For this purpose we proposed a path vacant ratio which finds a set of link-disjoint paths from the available paths. A load balancing and congestion control algorithm is proposed to adjust the load over multipath. A threshold sharing algorithm is proposed to divide the packets into segments that will be delivered to destination based upon the path vacant ratio. Simulations demonstrate the performance of the adaptive and secure load-balance routing scheme.

Keywords: wireless sensor networks (WSNs), service oriented architectures, Load balancing, multipath routing protocols, congestion control

I. INTRODUCTION

The wireless sensor networks have the ability to change the way to gain information for many applications and interact with the world [1]-[5]. The existing WSNs are designed for definite purposes and lack of standard operations and representation for sensor data can be used by upper layer applications or services. Service oriented architectures are proposed to support the interaction between different applications [4], [6], where functionalities are treated as services e.g., data aggregation service, data processing service, and localization service [7], [8]. The aims of the service oriented WSNs is combining different technology with independent service provisioning where the applications are treated as services. How to improve the throughput of WSNs is a critical challenge in the design of service-architectures [2], [3]. For this purpose it is suitable to design an adaptive multipath routing scheme that is able to reduce the traffic and also supports the OS requirements and achieve a reliable path from source node to destination node. In this paper, a multipath routing scheme is proposed, which have the following features 1) Application independence; 2) Secure delivery of data; 3) Adaptive congestion control and rate adjustment and 4) Extensibility. An adaptive and secure load-balancing routing scheme is proposed which improves the network performance for service oriented WSNs. Most existing multipath routing protocols do not achieve the service-oriented architecture over WSNs. To treat each application as a service link-disjoint-based multipath routing is a good idea. The service oriented WSNs should avoid forwarding messages to unrelated nodes it should search service related nodes only to them forward the routing message. The remainder of this paper is as follows. Section II related works, In Section III, the congestion control scheme is proposed for multipath. Section IV describes the secure multipath load-balancing routing scheme, and Section V reports the simulation results and analysis. Section VI describes conclusion.

II. RELATED WORKS

Multipath routing protocols such as Ad hoc on demand multipath distance vector (AOMDV) [21], On-demand multiple route maintenance in AODV extensions (ORMAD) [23], Temporally Ordered Routing Algorithm (TORA) [22] and interference-minimized multipath routing (I2MR) [24] are the common examples of ad hoc networks. AOMDV is an extension of ad hoc on-demand distance vector (AODV) that supports multipaths by providing the number of link disjoint and loop free path where the control packet of AODV is redesigned and an advertising hop-count field and a route-list field are added. Similarly, ORMAD is a novel approach and a link-disjoint extension of TORA. TORA is an distributed and adaptive routing algorithm that provides multipaths by maintaining and building a directed acyclic graph at a destination. When links are broken, In TORA, a local repair procedure will be invoked at the upstream node. The ORMAD optimize the overhead of the routing in path discovery and maintenance stages. In 12MR it supports high rate streaming and also it minimizes the interference over multipaths. In congestion control scheme 12MR does not address the problem of robustness and security where the first source node delivers a packet on the main path and then delivers the next packet on the second path after two packet transmission intervals. This process continues until all the packets in the queue are transmitted. In 12MR of load balancing scheme, the packet loss on primary and secondary path may cause delays. Load balancing algorithm is proposed by Lu and Suda which is based on balanced tree structure. The routing tree can more effectively balance the load then the shortest-path and breadth-first routing schemes. Most of the existing multipath routing schemes suffer from the following four problems

- A packet-distributing scheme at the source node results in security problems.
- Because of the susceptibleness of service-oriented WSNs, according to the rate on disjoint paths the load over the multipaths must be balanced.
- In WSNs, congestion may decrease the usage of channel and cause the packet loss which will lead to drop the packet and long packet delay.
- A multipath evaluation metric is still lacking.

In this paper, we will address the challenges and present a secure and adaptive load-balancing multipath routing protocol based on AODV, namely, service-oriented multipath AODV (shortly as SM-AODV), which includes the following features.

- A novel technique is proposed by considering the security of data delivery. It is the first phase of our adaptive load-balancing multipath routing scheme to improve the data confidentiality in the service-oriented WSNs.
- The path vacant ratio of multipaths is computed by a load-balancing approach is proposed for multipaths. The path vacant ratio can be used to evaluate the load over multipaths.
- To adaptively adjust packet delivery rate over each path an adaptive congestion control scheme is proposed, according to the congestion level that maintained in the HELLO message.

III. CONGESTION CONTROL SCHEME FOR MULTIPATH

Multipath discovery and maintenance is used to find out multipaths between source node to destination node. A link-disjoint path can be easily found out by the method stated in [21]. In link-disjoint paths, the failure of a link will cause the failure of single path. Here route discovery procedure is used to find a set of link disjoint and loop free paths. The duplicate copies of the (RREQ) which arrived at the intermediate nodes are not immediately discarded and all received RREQ messages are recorded in an RREQ table. To find a new node-disjoint path to the source node, each intermediate node checks each copy. If a new node-disjoint Path is found, and then the node will further check that the reverse path can be set up, if so, valid path is established, and the destination node will send an routing reply (RREP) message for all received RREQ. In this case, the intermediate node will forward the received RREP to the nodes listed in the RREQ table along with the shortest path to the source node. By this way, multipaths can be found.

A. Congestion Control

Based on buffer occupancy as well as the wireless channel load, congestion detection technique is used to detect the congestion. The congestion control scheme for multipaths includes the following three stages: 1) congestion detection; 2) congestion control and notification; and 3) congestion cancellation and load adjustment. Congestion control scheme is proposed, which adaptively adjust the load over the multipaths and reduce the congestion to avoid loss of packets and thus improve the throughput, reliability and security of traffic. The proposed congestion detection scheme can provide service ratio and congestion notification when it occurs. According to the value of, congestion is divided into four levels: 1) No congestion for 1 ≤ pk(r); 2) Light congestion for 0.8 ≤ pk(r) ≤ 1; 3) Congestion for 0.4 ≤ pk(r) < 0.8 (in this situation, the node will send a CONGEST message to its parent nodes on the path Lmij); and 4) heavy congestion for pk(r) < 0.4 (under this situation, the node will send a RESCHEDULE message to its parents). The details can be found in Algorithm 1.

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 f(CongSent) == TRUE then
        switch(CONGEST_LEVEL)
        case 0: break;
        case 1: break;
        case 2: AdjustLoad();ResetFWM();break;
        case 3: AdjustRate();ResetFWM();break;
        default: break;
    end
end
```


B. Congestion Control and Notification for Multipath
To tune the congestion on multipaths, hop-by-hop rate adjustment mechanism is used. The scheduling rate is defined as how many packets are scheduled at a time interval from the priority queue on the path, as shown in Fig.1.

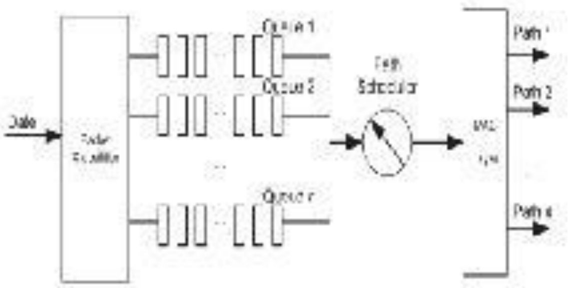

Fig 1. Congestion Path Schedule

C. Congestion Cancellation and Load Adjusting
To allow the current data packet to be transmitted before sending the CONGEST message to the source node, the congestion cancellation procedure empties its buffer and reduces the amount of backlogged data packets.

```
Algorithm 2 Adjustment Algorithm

Input: Current rate
Output: Adjust delivery rate
Check the CONGEST message:
if (CheckForCongestion() && (ConfigSend ==
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
```

IV. SECURE MULTIPATH LOAD-BALANCING ROUTING SCHEME IN WSN.

SM-AODV includes three phases: packet delivery scheme, multipath evaluation and scheduling scheme, and congestion control scheme.

A. Phase One: Packet Delivery Scheme
The threshold secret sharing algorithm is used to split the data into multiple shares. Each share is packed into an AODV packet, as shown in Fig. 2.

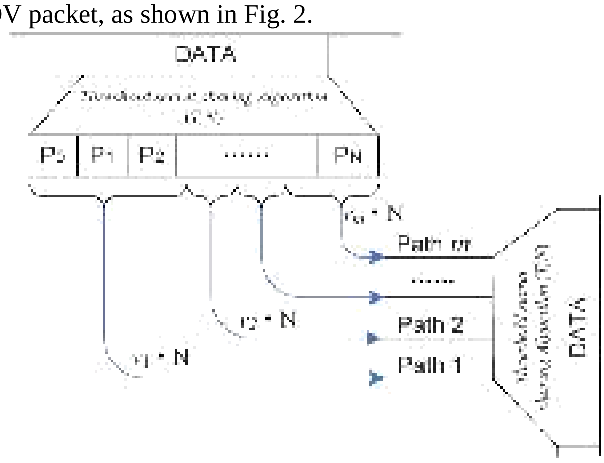

Fig 2. Packet Delivery Scheme

If the data is split into N packets, it can be recovered from any received *T* out of *N* packets. This is called threshold secret sharing scheme which is denoted as (*T*, *N*), Where T is the threshold.

B. Phase Two: Multipath Evaluation and Scheduling
Based on AOMDV, multipath is classified into multiple levels based on path vacant rate.

- Multipath Discovery: SM-AODV finds non disjoint paths.
- Evaluation of multipath load balancing.
- According to the threshold secret sharing algorithm, we need to split the load.
- According to the path vacant rate, load is distributed on multipaths.
- Congestion control module will be set up to monitor the CONGEST events. If CONGEST events arrive, then congestion control mechanism is invoked and according to the CONGEST_LEVEL, load will be scheduled.

TABLE I
SIMULATION PARAMETERS

Simulation Time	150 sec
Simulation Area	1000*1000m
Transmission Range	120m
Number Of Flows	10
Traffic Type	CBR
Packet Size	512 bytes

 ISSN (Online): 2347 - 4718

Packet Rate	4,8,12,20 packets/s
Number Of Nodes	100

C. Phase Three: Congestion Control

In this phase, each node checks the HELLO message to monitor the CONGEST event. When a node receives CONGEST events, it checks the value of CONGEST_LEVEL, if it's higher than one i.e. two or three, it means that load must be adjusted according to the CONGEST_LEVEL value. Some rules must be followed for adjustment, they are as follows:

- CONGEST_LEVEL = 0: The nodes do not do anything. It means that the path is not congested and every path is on its best status.
- CONGEST_LEVEL = 1: It means that the load is normal and each path is working well.
- CONGEST_LEVEL = 2: It means that the paths are congested. By reducing the sending rate it has to adjust the load.
- CONGEST_LEVEL = 3: It means that the paths are heavily congested and the multipaths must be updated.

V. SIMULATION AND PERFORMANCE EVALUATION

Figs. 3–6 show the performance of the proposed SM-AODV with different speeds of the nodes from 0 to30 m/s. Fig.3 shows the packet delivery ratio of the proposed protocols. Compared with AOMDV, the proposed SM-AODV shows a higher packet delivery ratio by reducing packet loss by up to 10%.

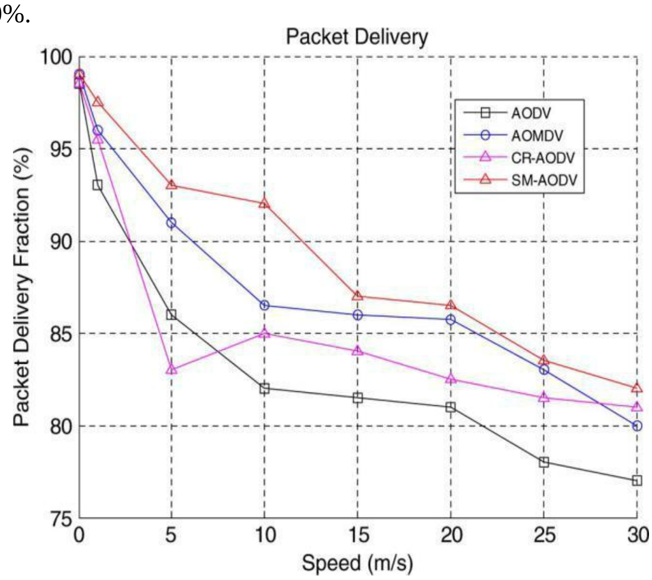

Fig 3. Packet delivery.

Fig. 4, we can see that SM-AODV shows a lower end-to-end delay than AOMDV by up to 5%. SM-AODV achieves less delay compared to others, which is because SM-AODV schedules the load on multipath.

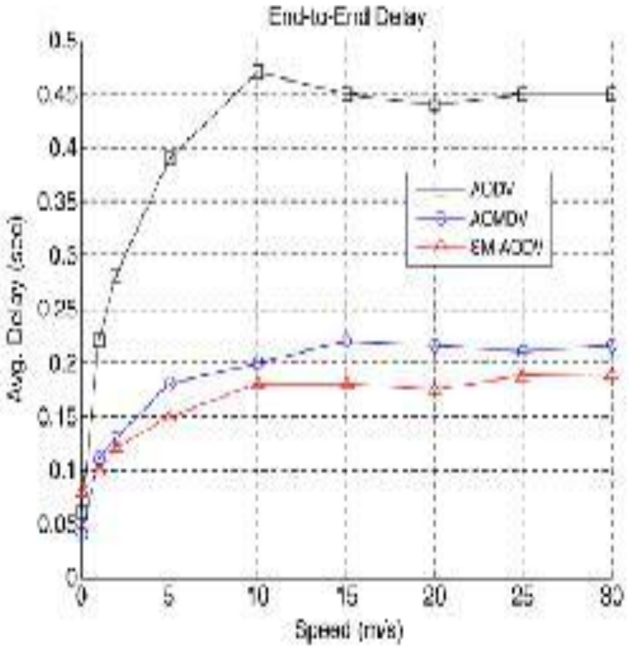

Fig. 4. End-to-end delay.

Fig. 5 shows the data loss ratio with different paths for AODV, AOMDV. SM-AODV achieves the lowest average data loss ratios.

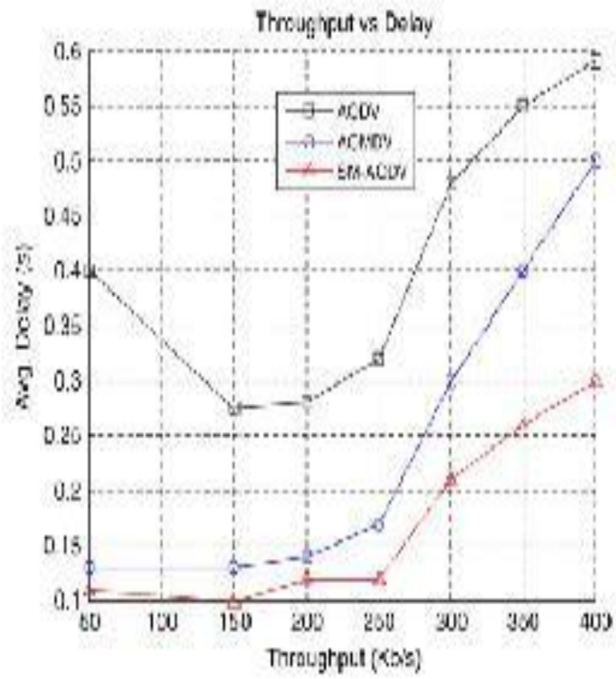

Fig. 5. Path data loss ratio with different paths.

Fig. 6 shows the average throughput of the three routing protocols. It can be seen that SM-AODV shows higher throughput than the other two protocols by up to 40%.

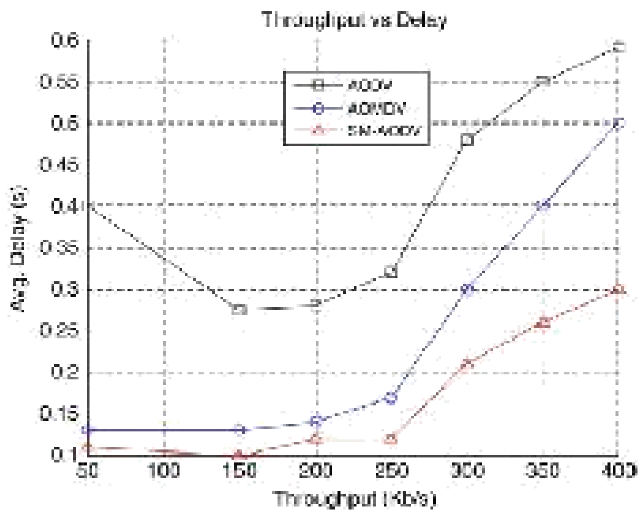

Fig. 6. Average delay versus throughput.

VI. CONCLUSION

To address the limitations of existing multipath routing schemes, an adaptive load-balancing multipath routing protocol (SM-AODV) uses load balancing, congestion control, and secure delivery scheme is developed. In SM-AODV, the packets are delivered across multipaths using a secure and reliable scheme, which unlinks the capabilities of the nodes and also offers a alternative optimization which are not available in the current systems. By using a secret sharing scheme at the source, SM-AODV achieves reliability in routing downstream traffic. SM-AODV uses an adaptive congestion control scheme, which is effective even in the case of node or link failure. This research gives the foundation for routing schemes over service oriented architecture, which is also expected to have the same impact on sensor architectures as service oriented systems had in the service systems .Here the nodes are capable of sensing and get the information as information collective service. This design provides effective performance for multipath and enables WSNs to provide reliable application-level services.

REFERENCES

[1] S. Li, X. Wang, and S. Zhao, “Multipath routing for video streaming in wireless mesh networks,” *Ad Hoc Sens. Wireless Netw.*, vol. 11, no. 1/2, pp. 73–92, 2011.

[2] T. Zhao, K. Yang, and H.-H. Chen, “Topology control for service-oriented wireless mesh networks,” *IEEE Wireless Commun.*, vol. 16, no. 4, pp. 64– 71, Aug. 2009.

[3] K. Lin, J. J. P. C. Rodrigues, H. Ge, N. Xiong, and X. Liang, “Energy efficiency QoS assurance routing in wireless multimedia sensor networks,” *IEEE Syst. J.*, vol. 5, no. 4, pp. 495–506, Dec. 2011.

[4] A.Rezgui and M. Eltoweissy, “μRACER: A reliable adaptive servicedriven efficient routing protocol suite for sensor-actuator networks,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 5, pp. 607–622, May 2009.

[5] X. Zhang and H. Su, “Network-coding-based scheduling and routing schemes for service-oriented wireless mesh networks,” *IEEE Wireless Commun.*, vol. 16, no. 4, pp. 40–46, Aug. 2009.

[6] L. D. Xu, “Enterprise systems: State-of-the-art and future trends,” *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 630–640, Nov. 2011.

[7] L. Duan, W. Street, and E. Xu, “Healthcare information systems: Data mining methods in the creation of a clinical recommender system,” *Enterprise Inf. Syst.*, vol. 5, no. 2, pp. 169–181, May 2011.

[8] K. Wang, X. Bai, J. Li, and C. Ding, “A service-based framework for pharmacogenomics data integration,” *Enterprise Inf. Syst.*, vol. 4, no. 3, pp. 225– 245, Aug. 2010.

[9] D. Chiang, C. Lin, and M. Chen, “The adaptive approach for storage assignment by mining data of warehouse management system for distribution centres,” *Enterprise Inf. Syst.*, vol. 5, no. 2, pp. 219–234, May 2011.

[10] E. Xu, M. Wermus, and D. Bauman, “Development of an integrated medical supply chain information system,” *Enterprise Inf. Syst.*, vol. 5, no. 3, pp. 385–399, Aug. 2011.

[11] L. Duan and L. D. Xu, “Business intelligence for enterprise systems: A survey,” *IEEE Trans. Ind. Informat.*, vol. 8, no. 3, pp. 679–687, Aug. 2012.

[12] L. D. Xu,W. Viriyasitavat, P. Ruchikachorn, and A.Martin, “Using propositional logic for requirements verification of service workflow,” *IEEE Trans. Ind. Informat.*, vol. 8, no. 3, pp. 639–646, Aug. 2012.

[13] S. Li, L. Xu, X. Wang, and J. Wang, “Integration of hybrid wireless networks in cloud services oriented enterprise information systems,” *Enterprise Inf. Syst.*, vol. 6, no. 2, pp. 165–187, May 2012.

[14] X. Chen, Y. He, and H. Huang, “An approach to automatic development of interlocking logic based on Statechart,” *Enterprise Inf. Syst.*, vol. 5, no. 3, pp. 273– 286, Aug. 2011.

[15] L. Li, “Introduction: Advances in E-business engineering,” *Inf. Technol. Manage.*, vol. 12, no. 2, pp. 49–50, Jun. 2011.

[16] S. Xu and L. D. Xu, “Management: A scientific discipline for humanity,” *Inf. Technol. Manage.*, vol. 12, no. 2, pp. 51–54, Jun. 2011.*IEEE Trans. Ind. Informat.*, vol. 8, no. 3, pp. 669–678, Aug. 2012.

[17] L. D. Xu, C. Wang, Z. Bi, and J. Yu, “AutoAssem: An automated assembly planning system for complex products,” *IEEE Trans. Ind. Informat.*, vol. 8, no. 3, pp. 669–678, Aug. 2012.

