國立交通大學

資訊科學與工程研究所

碩 士 論 文

無線感測網路中具可靠傳輸之路由協定

Reliable Routing Protocols in Wireless Sensor Networks

研 究 生：張振龍

指導教授：趙禧綠　助理教授

中 華 民 國　九 十 五　年 六 月

Abstract

Wireless sensor networks are characterized by limited resources including energy and bandwidth. By equipping different sensing units and deploying those sensor nodes in a specific region, more and more applications are able to be carried out. These applications may require different bounded latency, successful delivery rate, or data redundancy for the data in order to provide Quality of Service (*QoS*) to the sensor networks. Applications like fire detection will require delivering packets in different priorities since the sensed event with higher temperature is more important than a normal one. Packets with higher priority should be delivered in a more reliable way. In this thesis, we propose two reliable routing protocols for wireless sensor networks which can provide reliability to the packets by maintaining single and multiple reliable paths. The procedure of maintaining multiple paths can also reduce the routing overhead and thus prolong the lifetime of the network. From the simulation result, the packet delivery rate of our protocol performs well under different reliability demand and has smaller routing overhead due to the multiple paths maintenance.

摘要

無線感測網路的最大特性為受到限制的資源(resource-constrained)，包含能源以及頻寬。藉由在每個感測節點配置不同的感測元件並且將感測節點散佈在欲觀測之特定區域中，越來越的多應用得以付諸實行。這些應用為了在無線感測網路上提供服務品質保證(Quality of Service)，對於資料的傳輸可能會有不同的要求，包含有延遲限制、傳送成功率、或資料重複性。 一些像火災感測的應用便需要將感測的資料依照不同的優先權去處理，因為感測到比較高溫度的事件比正常溫度的事件更為重要。具有較高優先權的封包需要以比較可靠的機制去傳輸。在此篇論文當中，我們提出了兩個應用在無線感測網路上的可靠路由協定，藉由維護單條及多條到達目的地的可靠路徑，我們將可以依照封包的可靠需求提供相對應的可靠度。 維護多條路徑的程序也可以降低整體在路由之額外負擔。 模擬結果顯示，我們所提出的路由協定在不同的可靠需求當中，藉由維護多條可靠路徑，封包傳輸成功率以及路由之額外負擔均有比較好的表現。

致謝

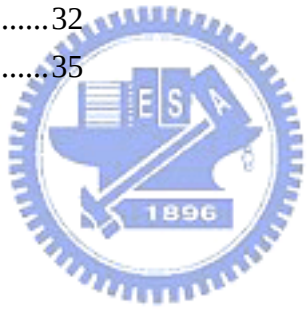
能夠來到台灣一流學府—國立交通大學攻讀碩士班不僅是我的人生志願，同時也是家人對我的滿心期待。當初在長庚大學電機系就讀時，成績不甚理想，對於自己的未來以及學業表現皆無任何企圖心。靠著班上同學在考研究所的團結一致、努力不懈，許多同學得以金榜題名，錄取國立大學研究所。

緊接著轉換學習環境來到交通大學，不同的上課步調、學習方式，以及從電機系轉到資訊系的程度落差，讓我一開始手足無措。更由於要補修兩門資訊相關課程，修課就讓我吃盡苦頭。靠著實驗室同學的傾囊相助終於讓我跟上進度，修課成績也得以進步許多。

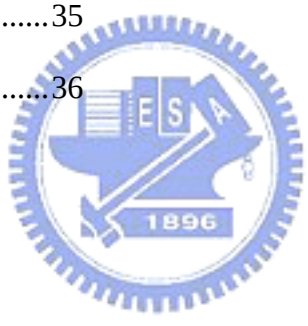
本論文的完成，首先要感謝我的指導教授—趙禧綠教授。靠著研讀 Paper 以及老師給予的觀念指導，讓我能夠在修課壓力之下繼續我的論文研究。從決定論文題目、定義所要解決之問題以及方法、模擬分析、以及最後的論文撰寫，中間所要付出的努力以及遇到的挫折是前所未有，惶恐的我，藉由老師的耐心指導以及技巧傳授，論文也漸漸的有了雛形。寫程式一直是我的弱點，模擬的完成，要特別感謝實驗室同學的幫忙，謝謝他們具有無比的耐心教導我程式技巧。與老師以及實驗室同學度過兩年的碩士生涯，獲益良多，很感謝他們造就我的進步以及帶給我一段很豐富的生活。

最後，要特別感謝我的家人，沒有他們，上面三段文字都不會出現。感謝父母為了讓我有成就所付出的一切，感謝爸爸總是帶領著我前進，為我規劃出美好的人生，感謝媽媽帶給我的溫暖，讓我總是很急切的想回家。對於所有曾經幫助過我的人，真的非常感謝妳們的付出。

Contents



List of Figures



List of Tables

Chapter 1.
Introduction

1.1 Wireless Sensor Networks

Wireless sensor networks (WSNs) is a brand-new field for people to carry out more applications in sensing technique. In particular, due to the great improvement in MEMS-based technology, low power and small size of SOC, VLSI technology, and low power RF design in recent years, sensor nodes are capable of containing very complex and powerful circuits in small volume. Each sensor node is composed of sensing devices, low power CPU, memory, antenna, signal processing units, batteries, and so on. Users can fabricate those sensor nodes base on the demand of the applications.

The most important characteristic of wireless sensor networks (WSNs) is the small size of the sensor nodes. With the characteristic, we can deploy those sensor nodes in a large field to sense the target we are interested in. But this characteristic also brings out the limitation in designing the wireless sensor networks-“Resource Constrained”. The goal is to make the cost smaller and thus prolong the lifetime of the network.

Wireless sensor networks and ad hoc networks have many aspects in common. They are both fully distributed and multi-hop wireless networks, and both are formed in an “ad hoc” manner. They are both supplied by limited power unit. But the wireless sensor networks have much more designing issues in saving power since the network lifetime are expected to be over several months or several years with using only one or two batteries. Once those small ”smart dust” are deployed in the area, it is not

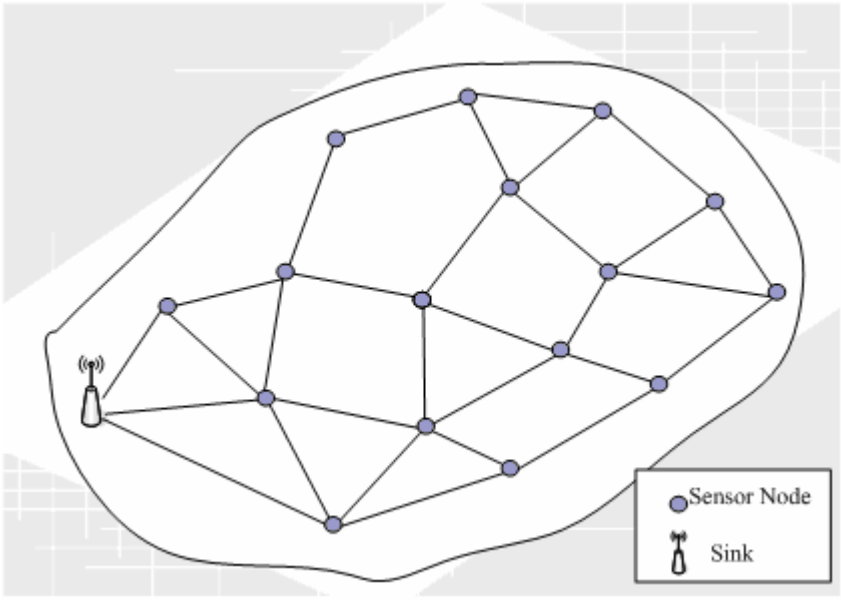


Figure 1-1 Infrastructure of WSNs

feasible to recharge them if their power were exhausted. It is also expected to provide dynamic forming topology, fault-tolerance, and high flexibility.

Depends on the application, a wireless sensor network usually contains a sink node which is connected to an existing communication infrastructure or the Internet and many sensor nodes which are randomly deployed in a large area, as Fig. 1-1 shows. A sink node is the node which generates the query message and receives sensing information from sensor nodes. With the unique characteristic of wireless sensor networks, more and more applications will be made possible to achieve.

1.2 Applications over Wireless Sensor Networks

Protocol design in wireless sensor networks is basically depend on the application itself. According to different scenario, protocol should be designed to match the situation. Such as target tracing may need the location-aided protocol to get the accurate position while the temperature sensing system may need the data aggregation technique instead of the accurate positioning technique. By equipping

different sensing units, sensor network can be applied in numerous applications. The following are some application examples of wireless sensor networks:

(1) Detecting object: The earliest idea of wireless sensor networks is used to monitor the battle field surveillance. Once we deploy those sensor nodes in random fashion or in manual fashion, the sensor nodes may used to detect the presence of alliances or enemies. With the information returned by the sensor nodes, military could obtain the information easily in the tough situation.

(2) Monitoring the nature: Sensor networks can be used to detect the difference of temperature, moisture, noise, vibration…etc. If can also measure the displacement of the mountainside if a GPS or location aided protocol is provided.

(3) Medical treatment usage: Each patient may equip several sensors to record the blood-pressure, heart beat, body temperature, and so on. Even if the patient is moving, those sensor nodes can report data to the central system as usual.

(4) Biological observation: For animals living in a group such as cattle, a shepherd can monitor the amount of the cattle in a pasture and record the readings of their healthy.

(5) Critical event detecting: A fire accident in a building could be reported in the most efficient way to reduce damage. Also it can provide feedback information to air conditioner to maintain constant temperature.

These applications have some challenges to overcome with regard to hardware, topology, and protocols design. Since each sensor node is expected to be robust and long-lived under different environments, this can be achieved by enhancing the efficiency of the hardware, such as battery capacity, accuracy of the sensing unit,

consuming power of the antenna, and the control board. Regardless the improvement in hardware design, the performance of the WSN is greatly influenced by the topology and protocol operations. Topology control [15], [16], [17], [18] in WSNs is another important issue to save power and report data efficiently. Protocol design includes the link layer protocol, routing layer protocol, transport layer protocol, etc. According to different applications, these protocols can provide energy-efficiency, reliability, or minimum overhead. In this thesis, we focus on the routing protocol design for wireless sensor networks.

1.3 Routing Challenges in Wireless Sensor Networks

Under different scenarios, the goal of designing a routing protocol in wireless sensor networks can vary a lot. Despite the common challenges with Ad Hoc networks, such as consuming minimum power and minimum overhead, WSNs have more unique designing issues that need to be considered. The following shows the challenges and issues about WSNs:

(1) Node Deployment: Since the sensor nodes are deployed in distributed and random/manual fashion, different deploy methods may influence the performance of the routing protocol a lot. Most of the routing protocols are sensible about the connectivity and coverage degree of the nodes. If the resultant topology can not provide enough connectivity or coverage density, those protocols may result in bad performance. Self-configured is necessary for wireless sensor networks. Once those sensor nodes are deployed in the region, they have to configure themselves, including startup, sensing, building neighbor information…etc.

(2) Data Reporting Method: According different application, data reporting can

be categorized as time-driven(periodic), event-driven(on-demand), query-driven(on-demand) or a hybrid version of those methods. Routing protocols are highly influenced by data reporting methods in terms of energy consumption and routing overhead.

(3) Fault Tolerance: Wireless sensor networks are designed to apply under different environment, some of them might be very difficult such as battle-field and the forest. Sensor nodes may lack of power or the link may be noisy. It is very important to provide a reliable and consistent routing protocol for sensors to handle those situations. If the network is dense enough, MAC protocols, such as SMAC [12], which schedule the nodes into sleeping, idle, and wake-up states cooperating with reliable routing protocols, can result in better performance in fault-tolerance.

(4) Scalability: Unlike Ad Hoc networks, the amount of sensor nodes may be up to hundreds or thousands. So designing a scalable routing protocol is also an important issue. With the amount of nodes increases, the routing overhead should be under a certain limit.

(5) Data-Centric Routing and Data Aggregation: The generating data in wireless sensor networks is mostly based on the query broadcasted from the sink node. Only nodes who have sensed useful event should report the information to the sink. Basically, nodes in close neighborhood may sense the event similarly. Data aggregation is needed in dense deployed wireless sensor networks to reduce the traffic redundancy.

(6) Quality of Service (QoS): Like the Ad Hoc networks, wireless sensor networks would need QoS for different data priority in specific applications. Some data may be useless after certain time periods or may be more important than normal one; data with greater variance is also more critical

than smaller one. So a routing protocol providing quality of service should forward these packets in a different manner.

(7) Power efficiency: Each sensor node is powered by few batteries and the lifetime of the wireless sensor network is expected to be several months at least. Prolonging the lifetime of the WSNs has always been the main objective in most protocols. It can be done by reduce the routing overhead, forming clustering, topology control, or applying data aggregation,…etc.

1.4 Motivation

Energy-efficiency is the primary considered issue in designing wireless routing protocols. Many protocols have been proposed to provide energy efficiency such as [3], [4], and [5]. They propose different mechanisms such as local route repair, number of retransmissions, and data aggregation to reduce the overhead and energy consumption.

However, the goal of the wireless sensor networks is to report information back to the sink effectively. Some applications would require routing protocol to provide reliability for the data instead of minimizing the energy consumption. [8] has analyzed about the trade-off between traffic overhead and attained reliability; in order to provide enough reliability, some additional overhead is required to maintain the reliability demands. [9] Proposed a routing protocol called Efficient and Reliable routing protocol (EAR) which uses single path forwarding mechanism to route the packet. By setting different routing metrics, EAR can find a more reliable route according to the route score of each route to the sink if the packet requires a more reliable route instead of minimum hop count.

Many reliable routing protocols use multi-path forwarding mechanism for data

packets to increase end-to-end successful transmission probability such as [6], [10], and [1]. Considering the wireless sensor network, link failure and node failure may happen frequently under the unstable environment. So multi-path forwarding mechanism can provide more fault tolerance against the failure than single path forwarding does. The objectives are to increase the reliability while maintaining minimum overhead and energy consumption.

1.5 Organization

The rest of this thesis is organized as follows: Chapter 2 describes the related work about wireless routing protocols, including AODV[11] and AOMDV[10]. Chapter 3 introduces our proposed reliable routing protocol and an AODV-based routing protocol with reliability support. Performance evaluation and analysis is presented in chapter 4. The conclusion and future work are drawn in chapter 5.

Chapter 2.
Related Work

2.1 Ad hoc On-demand Distance Vector Routing

The Ad hoc On-demand Distance Vector (AODV) routing protocol [11] is a reactive routing protocol which can provide quick adaptation to dynamic link conditions, low processing and memory overhead, and low network utilization in wireless networks. Comparing to proactive routing protocol, reactive routing protocol is more suitable for wireless sensor networks because it consumes less network resources and maintains only useful routing information in each node. Since wireless sensor networks and ad hoc networks have many aspects in common, many proposed routing protocols in wireless sensor networks are based on the route discovery process discussed in AODV.

2.1.1 Message Formats and Routing Table Structure

There are four control message types defined by AODV, these control packets are used to find routes for the destination if a node is lack of the information to the destination or used to maintain the routing information. The message formats shows in Fig. 2-1~2-4, Fig. 2-5 shows the routing table structure. The detail explanation of each field in these control packets are presented in AODV [11].

(1) Route Request (RREQ) is a control message used to request a route. Each time a node does not have a route to a particular destination, the node broadcasts a RREQ packet.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type=1	Flags	Reserved	Hop Count
RREQ ID			
Destination IP Address			
Destination Sequence Number			
Originator IP Address			
Originator Sequence Number			

Figure 2-1 RREQ Message Format of AODV

(2) Route Reply (RREP) is a control message used to reply the RREQ to the source. RREP is either sent from the destination node or the intermediate node which has fresh route to the destination.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type=2	R|A	Reserved	Prefix Sz	Hop Count
Destination IP Address				
Destination Sequence Number				
Originator IP Address				
Lifetime				

Figure 2-2 RREP Message Format of AODV

(3) Route Error (RERR) is an error message used to notify other nodes that the route to the destination is no longer exist due to link breaks.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type=3	N	Reserved	DestCount
Unreachable Destination IP Address			
Unreachable Destination Sequence Number			
Additional Unreachable Destination IP Address			
Additional Unreachable Destination Sequence Number			

Figure 2-3 RERR Message Format of AODV

(4) RREP-ACK is an optional control message for AODV used to acknowledge the RREP message.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5

Type=4	Reserved

Figure 2-4 RREP-ACK Message Format of AODV

(5) Routing table records some useful information for routing packets such as hop count and next hop. Sequence number is used to determine the freshness of this information.

Destination	Sequence Number	Hop count	Next Hop	Expired Timeout

Figure 2-5 Routing entry structure of AODV

2.1.2 AODV Routing Protocol Operation

(1) Maintaining Sequence Number

AODV provides loop-freedom of all routes by maintaining most recently heard sequence number of the destination. It is updated whenever a node receives new information from RREP, RREQ, or RERR messages. A destination node increments its own sequence number before it initiates a route discovery process or before it sends a RREP in response to a RREQ.

(2) Generating, Processing, and Forwarding Route Requests

A node will generate a RREQ if it requires a route to the specific destination which is not available in its routing table. Each intermediate node receiving this RREQ could either send a RREP if it has a fresh enough route or re-forwarding this RREP message.

(3) Generating ,Receiving, and Forwarding Route Replies

In each intermediate nodes on the path, any of them can send reply to

the source if having fresh enough route to the destination; otherwise, the destination generate a RREP after receiving first RREQ message. All the nodes being involved in this route discovery process will update the routing table information of the source node and destination node.

(4) Route Maintenance

AODV uses RERR packets to inform all the neighbors about route failures after the local route repair being unsuccessful; a node will also generate a RERR if it does not have a route for the incoming data packet. AODV maintains a neighbor-status table by sending hello message to all one-hop neighborhoods periodically to confirm the existence of each neighbor. Any hello replies would trigger the update process in the table. AODV also supports local route repair mechanism to rebuild the route without involving the source nodes. Although this mechanism might increase the path length, it can reduce the frequency of network-wide route discovery process and thus lower the network traffic load.

(5) Data Forwarding

Each time a source node has a data packet to send, it will first check the routing table whether there is any route to the destination. The data packet will be forwarded to the next hop directly if there is a valid route; if not, the source node will start the route discovery process and wait for a reply. The packet will be dropped after RREQ_RETRIES which is defined as 3.

2.2 Ad hoc On-demand Multi-path Distance Vector Routing

The Ad hoc On-demand Multi-path Distance Vector (AOMDV) routing protocol is a multi-path extension to AODV. It greatly reduces the routing overhead incurred by AODV and increases the packet delivery rate by maintain multi-path information to a destination in each route discovery process.

2.2.1 AOMDV Routing Protocol Operation

AOMDV uses the same control messages as AODV does. The goal of AOMDV is to provide disjoint and loop-free multiple paths from each source and destination pair in each route discovery process. AOMDV also adopts the sequence number mechanism to avoid the occurrence of route loop. Once a control packet with a higher sequence number is received, all the paths with the same smaller destination sequence number should be removed. AOMDV accepts incoming paths if their destination sequence number is identical. It also maintains an “advertised hop count” instead of “hop count” in AODV. Advertised hop count is the maximum hop count of all the paths in each route. For the situation receiving control packets with the same sequence number, it has two rules to follow:

(a) Route advertisement rule: Never advertise a route shorter than one already advertised.

(b) Route acceptance rule: Never accept a route longer than one already advertised.

By maintaining advertised hop count and following the two rules, AOMDV can permit more number of alternate paths to be maintained while ensuring loop freedom. The detail proof of the loop freedom is available in [10].

0 ~ 31 32 ~ 63 64 ~ 79 80 ~ 95 96 ~ 127 128 ~ 159 160 ~ 223

Destination A	Sequence number	Advertised hop count	Path list			
			Hop count1	Next hop1	Last hop1	Expiration timeout1
			Hop count2	Next hop2	Last hop2	Expiration timeout2
			…	…	…	…
Destination B	Sequence number	Advertised hop count	Hop count1	Next hop1	Last hop1	Expiration timeout1
			…	…	…	…

Figure 2-6 Routing Table Structure of AOMDV

The routing table of AOMDV is modified from AODV to accommodate more paths for each route, shown as Fig. 2-6. To maintain disjoint paths in each route, AOMDV adds extra field called “last hop” to each path. It has been proved that if each node maintains paths with different next hop and last hop, those paths are disjoint.

The route discovery process in AOMDV is very similar to AODV, but each intermediate node can send multiple RREPs to the source if it has multiple disjoint paths in the routing table; otherwise, it continues to forward the RREQ. If the destination receives the RREQ, it will update the destination sequence number and send RREPs back to the source. In AODV, the destination only replies the first received RREQ; however, AOMDV adopts a looser reply policy. The destination generates a RREP in response to every incoming RREQ if it has multiple loop-free reverse paths to the source. Such additional RREPs can increase the possibility of finding more alternate paths. Each node receiving the control packets can also update the path information. After one route discovery process, all involved node may maintain multiple paths to both the source and destination. Nodes will not initiate another route discovery process until all the paths to the destination are no loner available or have expired.

Every time a node has data packets to send, it will check the routing table for that destination. If the route is valid and has at least one unexpired path, AOMDV will choose the first path and forward the packet to the proper next hop; if no path is available, the node will initiate the route discovery process and wait for replies. Once the node generates RREQ for RREQ_RETRIES times and receives no reply, the packet will be dropped and declares as NO_ROUTE to the upper layer.

2.3 Discussion

Comparing to AODV, AOMDV performs well in end-to-end packet delay, packet delivery rate, and routing overhead. Since AOMDV maintains multiple paths to each destination, it always has alternate paths without re-generate RREQ message. This greatly reduces the frequency of global route discovery while providing fault tolerance to the network.

Consider the nature of WSNs, each sensor node has limited resources and will be deployed in an unstable environment. Design a reactive routing protocol with fault tolerance is necessary and, at the same time, consuming less resources of the networks and the sensor nodes. Obviously, AOMDV is more outstanding than AODV in all aspects if we want to develop a reliable routing protocol. Although AOMDV maintains multiple paths for each destination, it only uses single path to forward the packet. In other words, it provides fault tolerance to the node failure and link failure but not reliability to the data.

In the next chapter, we propose two reliable routing protocols for wireless sensor networks called SOMDV-R and AODV-R. The former is based on AOMDV which provides reliability to the data packets while achieves minimum routing overhead; the latter is modified from AODV in order to provide reliability to the data packet.

Chapter 3.
Reliable Routing Protocols in Wireless Sensor Networks

In this chapter, we propose two reliable routing protocols in wireless sensor networks called Sensor On-demand Multi-path Distance Vector Reliable Routing Protocol (SOMDV-R) and Ad hoc On-demand Distance Vector Reliable Routing Protocol (AODV-R). The former is discussed in Section 3.1; the latter is discussed in Section 3.2.

3.1 SOMDV-R

3.1.1 Protocol Overview

SOMDV-R is modified from AOMDV in order to provide reliability to the data forwarding. We define the reliability as “end-to-end successful transmission probability”. SOMDV-R shares several characteristics with AOMDV. They are both based on “on-demand and distance-vector” concept, hop-by-hop routing procedure, and multiple paths maintenance in routing table. The main difference lies in the estimation of reliable degree of each path and the data packet forwarding mechanism. Link quality of each node is required for SOMDV-R to calculate the path reliability. This information can obtain by hello drop rate in routing layer, beacon loss rate in MAC layer, or SNR ratio in physical layer…etc.

The goal is to design a protocol which is able to calculate the path reliability, and forward the packet according to the importance of each packet. Determine the importance of the generating data relies on the information-awareness technique; we skip this portion since it is out of the scope of this thesis. In order to maintain this

necessary information, using extra field in control packet header is needed. As we mentioned before, there is a trade-off between overhead and reliability; however, minimum overhead is also expected.

3.1.2 Routing Table Structure and Terminology

A. Routing Table Structure

The routing table structure is modified from AOMDV with only an extra field called "path estimation (*PE*)". It is a reference value of the reliability of this path and plays an important role in data packet forwarding. Fig. 3-1 shows the content of the routing table. Each field in the routing table is described in the following subsection.

B. Terminology

This subsection defines some terminologies used in SOMDV-R:

(1) Sequence Number (*Seqno*): It is a monotonically increasing number related to each destination in routing table. Higher sequence number means the relatively fresher information. It is updated whenever it receives a fresher control packet or it decides to initiate a route discovery for the destination.

0~ 31 32~ 63 64~ 79 80~ 95 96 ~ 127 128~ 159 160~ 223 224~ 287

			Path list				
Destination A	Sequence number	Advertised hop count	Hop count1	Next hop1	Last hop1	Expiration timeout1	Path estimation1
			Hop count2	Next hop2	Last hop2	Expiration timeout2	Path estimation2
			…	…	…	…	…
Destination B	Sequence number	Advertised hop count	Hop count1	Next hop1	Last hop1	Expiration timeout1	Path estimation1
			…	…	…	…	…

Figure 3-1 Routing table structure of SOMDV-R

(2) Advertised Hop Count (*Adv. HC*): It is the maximum hop count among all paths in each route, i.e. *Adv. HC* = MAX (HC_1, HC_2 …). It is used to determine the **Route advertised rule** and **Route acceptance rule** to avoid looping path as we discuss in Chapter 2.

(3) Reliability Demand of the source(RD_s): This parameter indicates the demand for the data delivery rate of the source. It is a value between 0 and 1 which representing the importance of the data. Determining the RD_s in each data packet is the technique about information-awareness which is out of the scope of this paper. We manually assign the RD_s in each data packet. By setting this value in the data packet header, SOMDV-R would forward this data packet according to its demand.

(4) Reliability Demand of the intermediate nodes(RD_i): Since RD_s would be updated in each intermediate node. We define this updated value as RD_i.

(5) Link Quality (Q_{ij}): It is the link quality between node i and j. Link quality is an essential information for estimating the path reliability. It is a value between 0 and 1 which is obtained by hello messages received from each neighbor in a time interval. Higher link quality means the link is better and more suitable for transmission. Link quality between node i and j can be calculated by:

$$Q_{ij} = \frac{H_{ij}}{S_{ij}} \quad (1)$$

, where H_{ij} is the number of hello messages node i has received from neighbor j and S_{ij} = number of hello message node i should receive from neighbor j in a time interval.

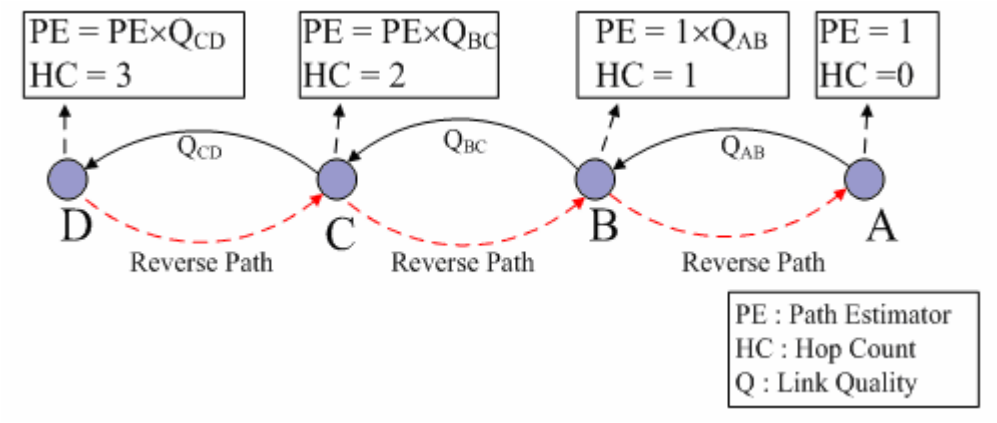


Figure 3-2 Calculation of PE and HC in each hop

(6) Path Estimation (PE): PE represents the reliable degree of the path. It is an estimating value between 0 and 1. The path with higher PE value means that it has higher end-to-end successful transmission probability. It is updated in each intermediate node as shown in (2) and Fig. 3-2.

$$PE(A \rightarrow D) = Q_{AB} \times Q_{BC} \times Q_{CD} \quad (2)$$

3.1.3 Protocol Operations

SOMDV-R consists of three components, i.e., route discovery, route maintenance, and data packet forwarding. The following subsections describe the operations of each component.

A. Route Discovery

In AOMDV, route discovery process is initiated whenever a traffic source node having a data packet to send with no valid path available in its routing table. SOMDV-R initiates a route discovery if the source node has no path in the routing table or has paths that can not satisfy the packet's demand. The traffic source then broadcasts a RREQ destined to the sink with initial hop count equal to 0 and path estimation equal to 1. Any intermediate nodes receiving this RREQ will update the hop count and path estimation in the control packet header, i.e., increment the hop count by 1 and multiply the PE by the link quality with the upstream node as shown in Fig. 3-2. After that, the node will form a reverse path toward the source node with the PE copied from the control packet header. This PE value means the successful transmission probability from current node to the traffic source.

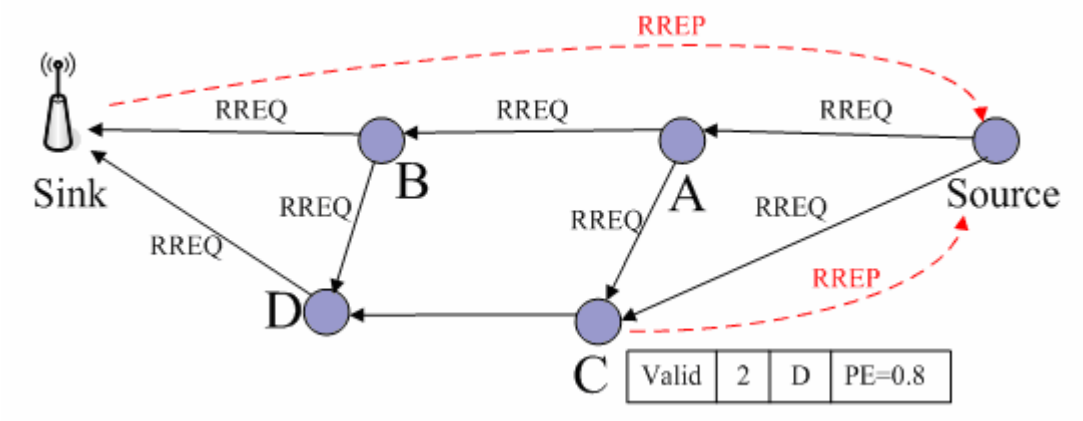


Figure 3-3 Sending Route Reply

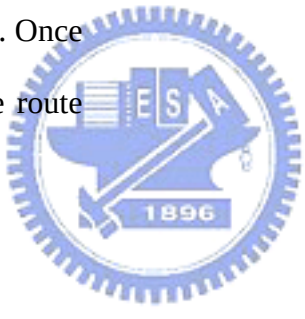
As shown in Fig. 3-3, any intermediate nodes receiving the RREQ will send an RREP back to the source via the reverse path if it has one or more valid and unexpired paths to the sink node (such as node C has a valid path to the sink with hop count equal to 2, PE equal to 0.8, and next hop D as shown in Fig. 3-3), the RREP represents a forward path that was not used in any other RREPs for this RREQ; otherwise, it simply re-broadcasts the RREQ if it has not previously forwarded any other copy of this RREQ(such as A, B, and D).

When the sink node receives a RREQ, it simply forms a reverse path as the intermediate nodes do and generates a RREP in response to every RREQ which arrives at the source via a loop-free and node-disjoint path. Any intermediate nodes receiving an RREP will update the packet header including hop count and PE value, update the routing table if necessary, and then forms forward path to the sink. After that, it will forward the RREP if there are any reverse paths that have not previously used for this route discovery; else, it simply discards the RREP.

After the route discovery process, the source node may receive multiple RREPs sent from disjoint paths. All the nodes involving in this route discovery process will also update the forward and reverse path information.

B. Route Update and Maintenance

SOMDV-R adopts the same route update and maintenance rules in AODMV. Each path has an expiration timeout field for the default lifetime of a path. The path will be purged if the timer has expired and the route will be marked as “DOWN” once all the paths are expired. Route update is invoked when a node receives a fresher control packet (including RREP, RREQ, and RERR) or receives a control packet with a shorter hop count and better PE to the sink node(including RREQ and RREP). Once updating the path information, the expiration timeout should be reset and the route



will be marked as “valid/invalid”, depending on the content of the control packet.

The local connectivity can be maintained either by link layer mechanisms or by routing layer mechanisms. In link layer protocols such as IEEE 802.11, each time a node receiving a CTS or ACK from a neighbor is able to confirm the connectivity. In routing layer, by proactively sending Hello messages to all immediate neighbors, SOMDV-R is able to maintain the local connectivity with each neighbor. Once a node can not receive any Hello messages from a specific neighbor for (ALLOWED_HELLO_LOSS × HELLO_INTERVAL), it will purge the neighbor from the neighboring table and declare the link as “broken”.

Depending on the distance of the broken link to the sink, route maintenance has two mechanisms:

(1) Local route repair mechanism is invoked if the intermediate node with a broken link is closer to the destination than the source node as shown in Fig. 3-4. The intermediate node D will buffer all the packets destined to the destination F and initiate another route discovery process. After receiving RREPs, the intermediate node D first updates the path information and then forwards all the buffered packets.

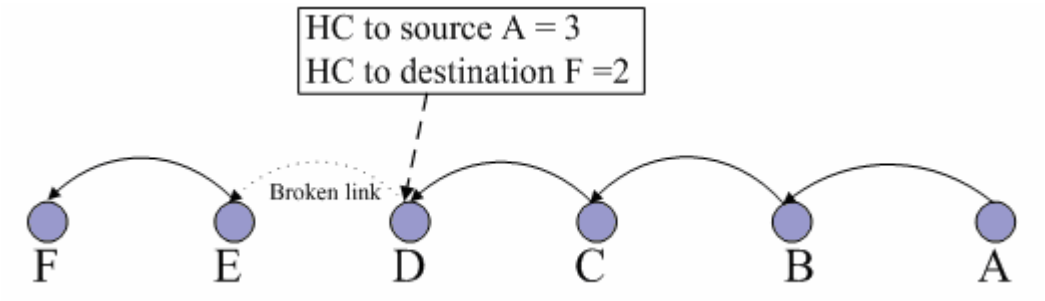


Figure 3-4 Local Route Repair

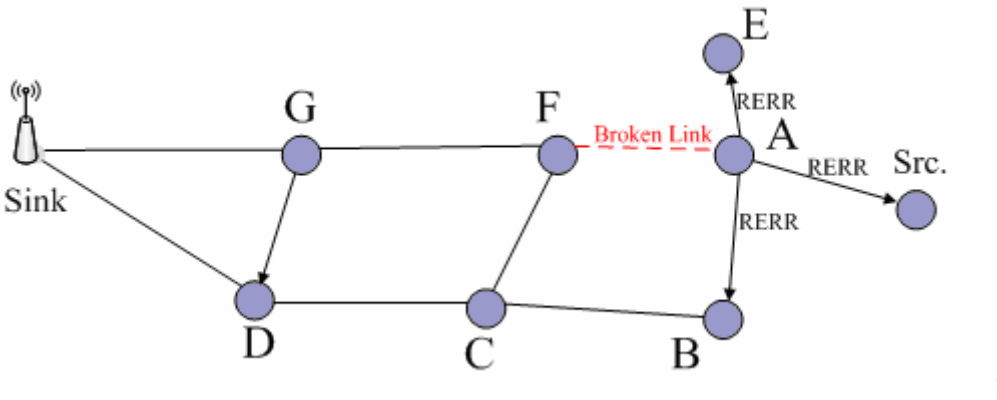


Figure 3-5 Forwarding RERR

(2) In Fig. 3-5, when the last path to the sink node of node A breaks and A can not initiate local route repair mechanism, i.e., the broken link is closer to the source than the destination, it will purge the route and locally broadcast a RERR to all its one-hop neighborhood (node E, B, and source). Each of its neighbors receiving the RERR will also purge the route if the last path to the destination does no longer exist and continue to forward the RERR to its immediate neighbors (node E). All the nodes having purged the route have to initiate another route discovery process if still needing the route to the destination.

C. Data Packet Forwarding

In the previous subsection, SOMDV-R establishes the basic knowledge of each path by route discovery process. Comparing to AODMV, data packet forwarding is more complex since the goal of SOMDV-R is to achieve reliability. In AOMDV, data packets are simply forwarded if there is at least one path to the destination; in SOMDV-R, we have to make the forwarding decision according to the relationship between *RD* and *PE* before we forwards each data packet.

The successful end-to-end transmission probability based on the local knowledge

of channel error rate is calculated by:

$$\text{Single path: } P(A \rightarrow B)=\prod_{j=1}^{h}(Q_{j,j+1}) \quad (3)$$

$$\text{Multi-paths: } P(A \rightarrow B)=1-\prod_{i=1}^{m}(1-\prod_{j=1}^{hi} Q_{j,j+1}) \quad (4)$$

, where m is the number of paths used to forward this packet, h_i is the hop count for path i. Once a sensor node senses an event according to the query from the sink, it will generate a data packet and assign a reliability demand (RD_s) value to the packet header before sending it. The RD_s and RD_i value plays a key role in taking the forwarding decision. The following Table I summarizes the cases when forwarding data packet.

Each forwarding node will first find the path with maximum *PE* value in the routing table and compare it with the *RD* value. If the *PE* value is bigger than the *RD* value, it means this path is suitable for forwarding this packet as the case 1 in Table I. So SOMDV-R uses single path mode to forward it, as the solid line shown in Fig. 3-6 (the dotted line means that it is an alternate path with PE_2). If single path is not enough for the packet's demand, SOMDV-R will forward the packet by multiple loop-free and node-disjoint paths, which means duplicating the packet and sending those duplicate packets via multiple paths, as shown in Fig. 3-7. The number of paths needed for this packet can be obtained from formula (4) and the upper bound of the

Table I. Forwarding Decision of SOMDV-R

Case	Destination	Reliability	Action
1	Available	Satisfied	Forwards the packet directly
2	Available	Unsatisfied	Keep forwarding
3	Unavailable	----------	Generate RREQ
4	----------	RD_i>1	Keep forwarding

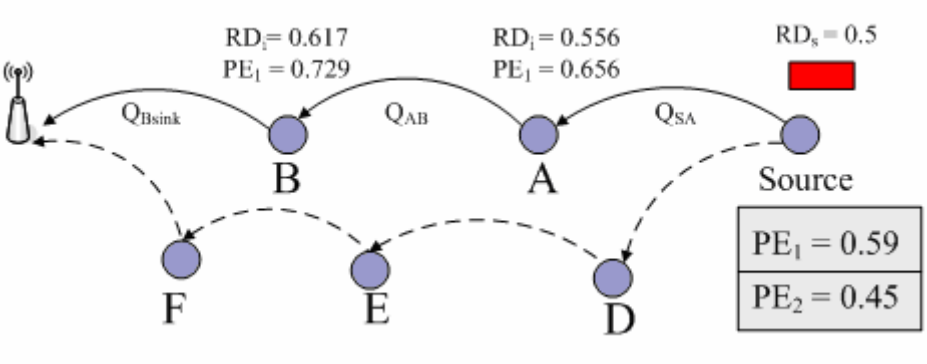


Figure 3-6 Forwarding packets using single path

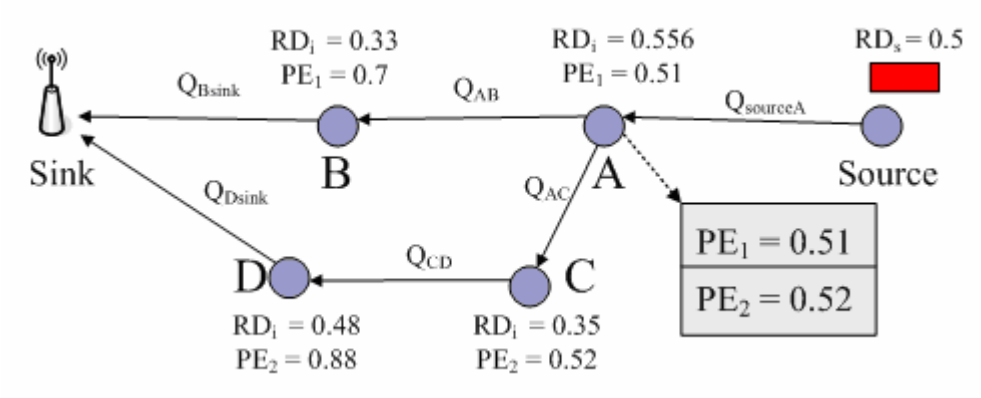


Figure 3-7 Forwarding packets using multiple paths.

number of multiple paths used to forward a packet is defined as MAX_Paths.

In Case 2, if the number of paths required to forward the packet exceeding MAX_Paths or if the number of paths in the routing table is not enough to satisfy the packet's demand, SOMDV-R would reset the RD_i in the packet's header as 0 and forward the packet via these multiple paths in order to increase the possibility of packet reaching the sink. In Case 3, the source node initiates the route discovery process if the route to the sink is not available.

Before forwarding the data packet, each intermediate node should adjust their hop count and RD value according to the reliability that the source expects it to provide from current node to sink as (5) and (6):

$$Hop\ \ Count\ =\ Hop\ \ Count\ +\ 1 \tag{5}$$

$$RD = RD / Q_{ij} \tag{6}$$

,where Q_{ij} is the link quality between the upstream node and the current node. In some quite unstable networks, the RD_i value may be over than 1 after updating if the packet has just traversed from a bad link, such as Case 4 in table I. Under this circumstance, SOMDV-R will never find any paths available for this abnormal RD, the better solution would be reset the RD_i as 0 and forward it via multiple paths.

If a node decides to use multiple paths to forward the packet, it should reassign the RD_i value in each duplicate packet's header. The main idea is to let the paths share the reliability demand and the paths with higher PE value responsible for more reliability. Fig. 3-8 shows an example if a node decides to use two paths with PE_1=0.6 and PE_2=0.3. After duplicating the packet, the RD_i value of each duplicate packet should be adjusted to RD_{i1} = 0.58 and RD_{i2}= 0.29 according to the ratio of these two paths. The following shows a simple calculation of this procedure:

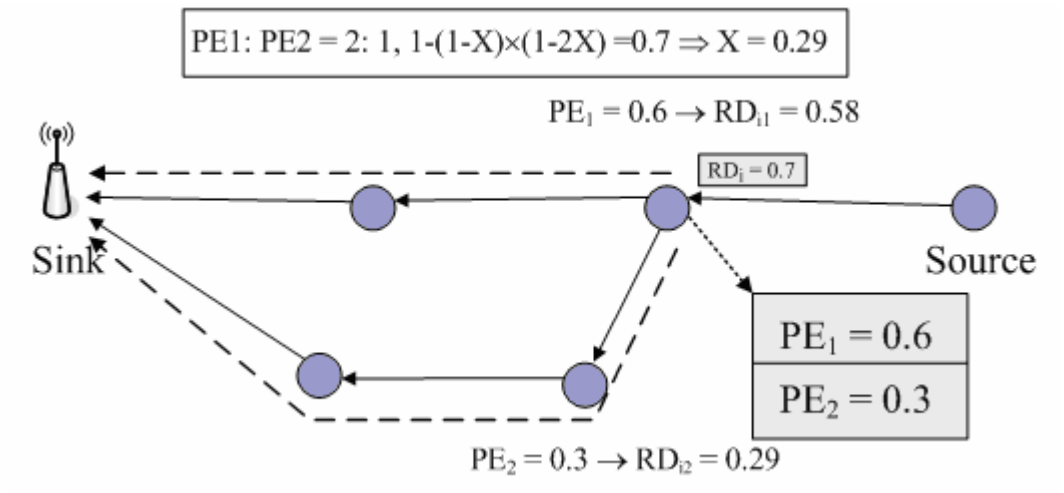


Figure 3-8 RD adjust mechanism

3.2 Modified Version of AODV: AODV-R

In this section, we modify the AODV routing protocol based on the mechanism of SOMDV-R. The only difference lies in the number of paths maintained for each route. The route discovery process of AODV-R is basically the same with SOMDV-R, including the flooding the RREQ with hop count and path estimation parameters. Each intermediate node having fresher route can send RREP back to the source. Once the first RREQ has been propagated to the sink, the sink will generate a RREP back to the source. The other duplicates of the RREQ would simply be dropped at the sink. The source could forward the packet if it has route to the sink and the PE value for the route is not less than the RD value in the data packet header; else, after RREQ_RETRY_TIMES, the packet would be dropped. In each intermediate node, if the route is not available or the route is not reliable enough, it would simply forward the packet via the unreliable path. We use AODV-R to compare with SOMDV-R about the overhead and the packet delivery ratio in the simulation.

Chapter 4.
Performance Evaluation

In this chapter, we evaluate our reliable routing protocol SOMDV-R, AOMDV, and AODV-R using ns-2 simulator [14]. The main objective is to observe the packet delivery rate of these three protocols under different channel error rate. Also, we show the relative overhead of forwarding a packet, the ratio of using single path, multiple paths, and no path.

4.1 Simulation Environment

We use a simulation tool based on ns-2 version 2.1b4a. Besides, IEEE 802.11 distributed coordination function (DCF) is used as the MAC layer protocol. We use the Lucent's WaveLAN radio model with the modified transmission range 150meters. 50 sensor nodes are randomly deployed in a 670m×670m square area. We set the sink node as the 51th node and all the nodes are static. Channel error rate is normally distributed between 0 and e_{max} across the area. It is used to simulate the channel error while receiving any types of packets and all links are bi-directional.

The Hello interval is defined as 0.5s which means that each node would locally broadcast two Hello messages in every second. We set the ALLOWED_HELLO_LOSS as two, i.e., if a node is unable to receive two continuous Hello messages from its neighbors within 2*Hello interval, it will remove the corresponding entity from its neighboring table.

We use 10 ~50 CBR connections with different RD_s in the simulations. These connections will last for 5 seconds with packet generating rate 0.5 pkt/s. Data packets

have a fixed size of 512 bytes. Each simulation is run for 60 seconds with the initial 5 seconds taken as the warm-up period to establish the link quality table. All connections start its traffic after warm-up. In each routing table entry, the number of paths maintained in each route is restricted to five. We set the MAX_Paths as two in our simulation.

4.2 Performance Metrics

We primarily consider the following four metrics:

(1) Packet delivery ratio (PDR): PDR is the end-to-end successful transmission probability calculated by the number of data packets received by the sink node dividing by the number of data packet generating in source node. PDR also represents the attained reliability in the protocol.

(2) Routing overhead: The control packets used in route discovery process and route maintenance such as RREQ, RREP, and RERR are routing overhead to the protocol. We define the routing overhead as formula (7):

$$\text{Routing overhead} = \frac{P_{control}}{P_{control}+P_{data}} \tag{7}$$

, where $P_{control}$ represents the amount of the control packets and P_{data} represents the amount of the data packets

(3) Mean latency: it is the average end-to-end latency for each successful transmission as formula (8):

$$T = T_{RD} + T_{PD} + T_{QD} \tag{8}$$

, where T_{RD}, T_{PD}, T_{QD} represent route discovery time, propagation delay, and queuing delay, respectively. When using multi-path, we consider the first duplicated packet with successful delivery only.

4.3 Simulation Results

4.3.1 Packet Delivery Ratio

Fig. 4-1 shows the PDR with varying channel error rate. We use 10 CBR connections without specifying packets' RD_s. In SOMDV-R, data forwarding is achieved by using single path without specifying any RD_s. In order to show the impact on PDR of a specific routing protocol, we use 10 connections which is a moderate load for the network to prevent the occurrence of buffer overflow. Since SOMDV-R is modified from AOMDV, with no reliability demand, our protocol has almost the same performance with AOMDV. From Fig. 4-1, it is obviously that the multiple path maintenance is more outstanding than single path maintenance in PDR. They both increase the PDR 10% more than AODV-R in average. The difference increases with the raising of channel error rate.

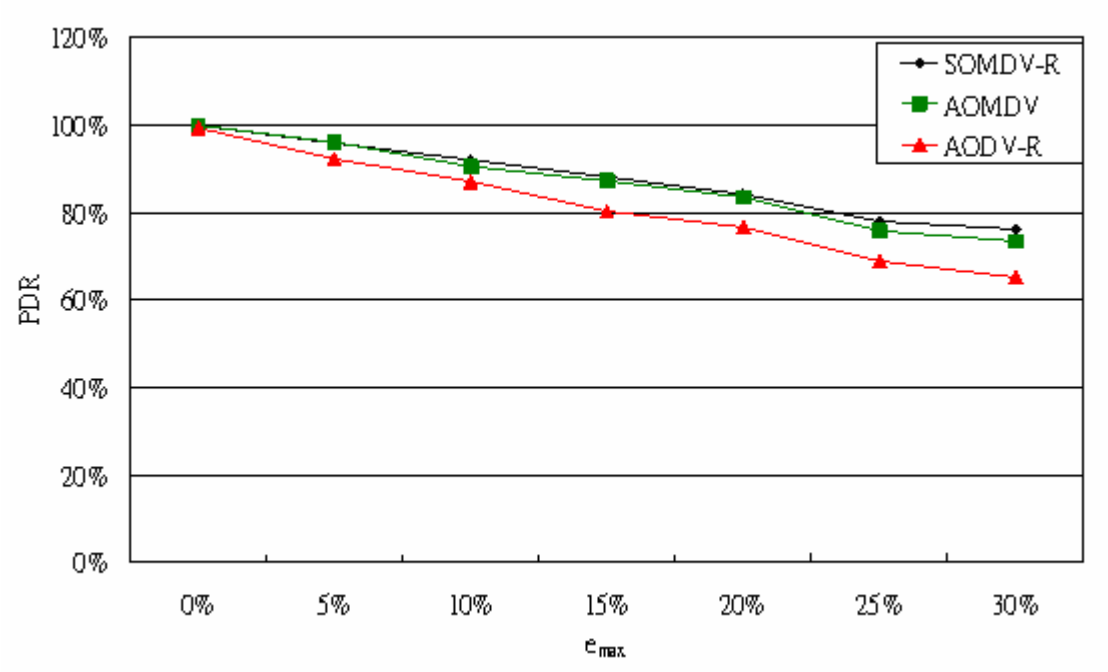


Figure 4-1 PDR with no RD_s

In Fig. 4-2, we simulate SOMDV-R and AODV-R with RD_s equal to 0.5 and 0.9 for each connection. Comparing to AODV-R, SOMDV-R has better packet delivery ratio due to multiple paths. For the curve of RD_s equal to 0.9 which is a quite high reliability demand, PDR of AODV-R drops suddenly if the channel error rate is larger than 10% while SOMDV-R has a smoother curve due to the multiple paths maintenance and data packet forwarding mechanism.

In the current progress, we restrict the number of multiple paths for forwarding packets as two. When the channel error rate is high, it is very difficult to find a reliable path even using two paths. There is a trade-off between reliability and overhead; if we want to provide high reliability in an unstable network, the overhead would be too high. High overhead is not expected in wireless sensor networks so we choose an appropriate and conservative number of multiple paths as two.

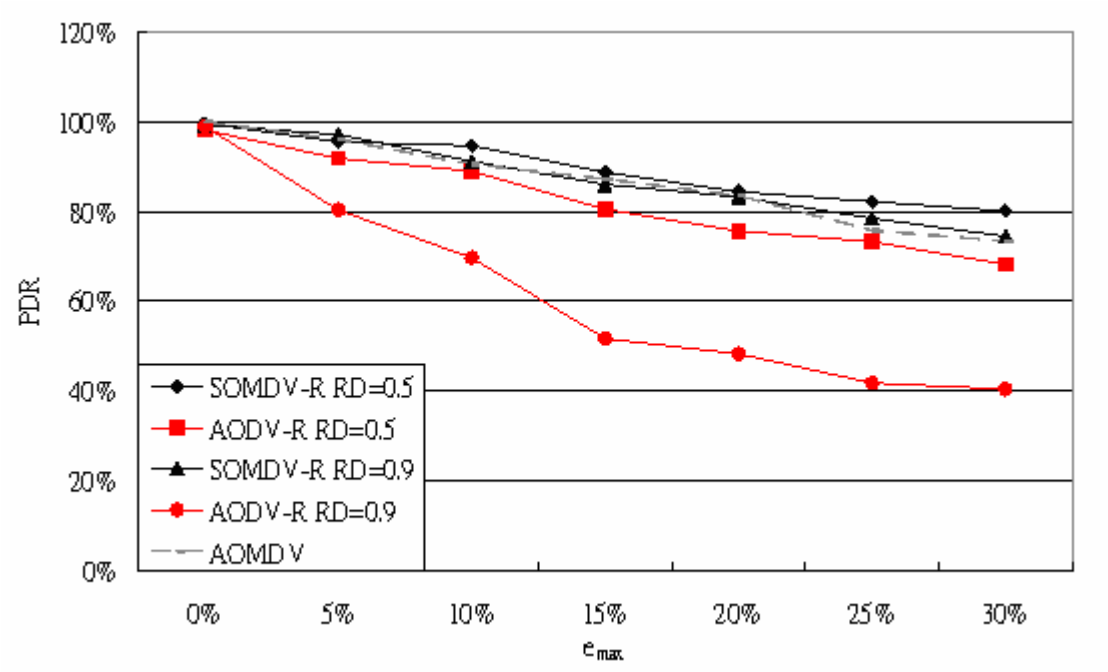


Figure 4-2 PDR with RD_s = 0.5 and RD_s = 0.9

We simulate different number of connections with RD_s varying from 0.1 to 0.9. The channel error rate is uniformly distributed between 0% and 20%. From Fig. 4-3, The PDR drops a little bit when the number of connection increases to 30. But SOMDV-R maintains high packet delivery ratio in all RD_s while the AODV-R drops severely when the reliability demand is over 70%. When the reliability demand is high, SOMDV-R shows the consistency in PDR by using multiple reliable paths forwarding mechanism. Under all cases of connections, SOMDV-R has better performance comparing to AOMDV since SOMDV-R always finds the more reliable path to forward the packet.

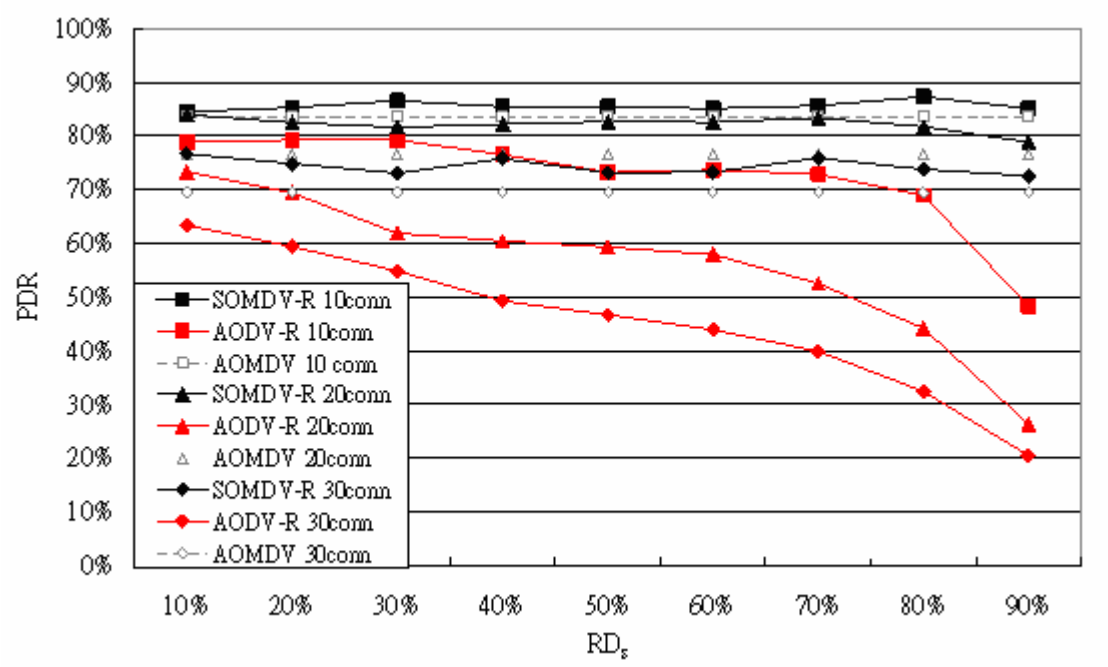


Figure 4-3 PDR with different RD_s

4.3.2 Overhead

Fig. 4-4~ 4-6 show the overhead with varying channel error rate. There are 10 CBR connections with different RD_s in each simulation. In Fig. 4-4, we simply evaluate the overhead without specifying any RD_s for AODV-R and SOMDV-R, and compare the overhead with AOMDV. Without giving any RD_s, AODMV and SOMDV-R have similar performance because they will not initiate another until no path being available in the routing table. This significantly reduces the frequency of route discovery process. While the channel condition becoming worse, the overhead increases because there is no usable path. In average, SOMDV-R reduces 10% overhead comparing to AODV-R.

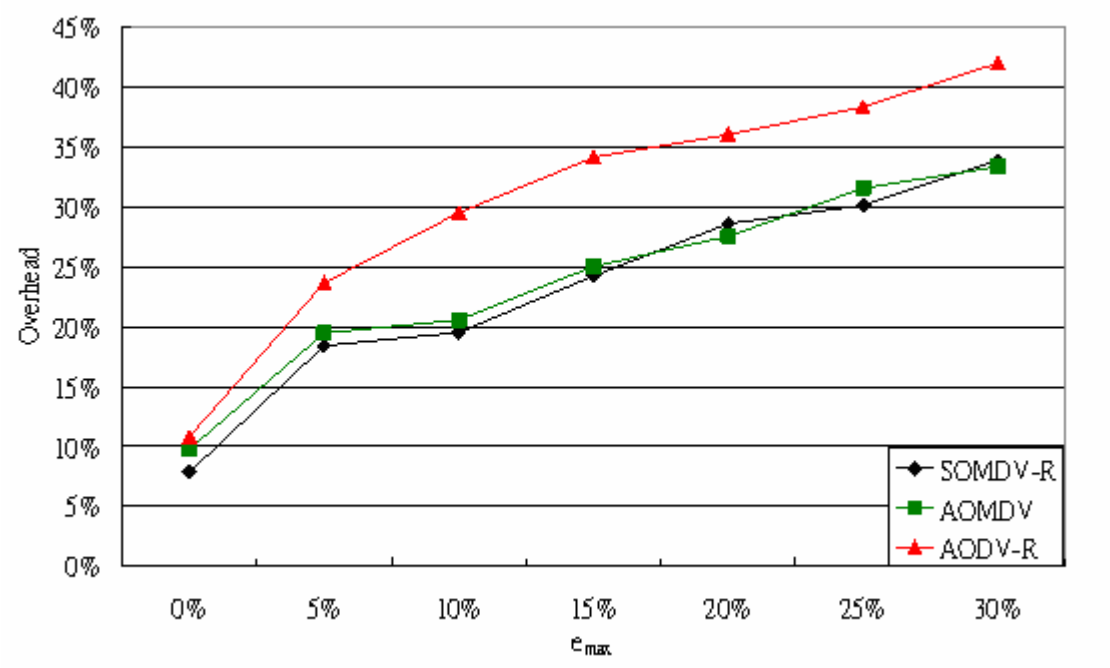


Figure 4-4 Overhead with no RD_s

Fig. 4-5 shows the routing overhead of SOMDV-R, AOMDV, and AODV-R. We set the RD_s as Random(0.2, 0.9) and 0.9 in the simulation. The overhead of SOMDV-R and AODV-R increases with the raising of the channel error rate since they both initiate route discovery process more frequently. But SOMDV-R has greater performance in reducing overhead while the channel error rate and RD_s is high. When the RD_s is fixed as 0.9 and the channel error rate is over 20%, AODV-R is not suitable for reliable forwarding since it always has no reliable path to use under unstable environment. The routing overhead of SOMDV-R increases only about 2% more than AOMDV when the RD_s is high. It is because SOMDV-R has to initiate more route discovery processes to find more reliable paths and there is always a trade-off between reliability and overhead. Even though, SOMDV-R minimizes the extra routing overhead.

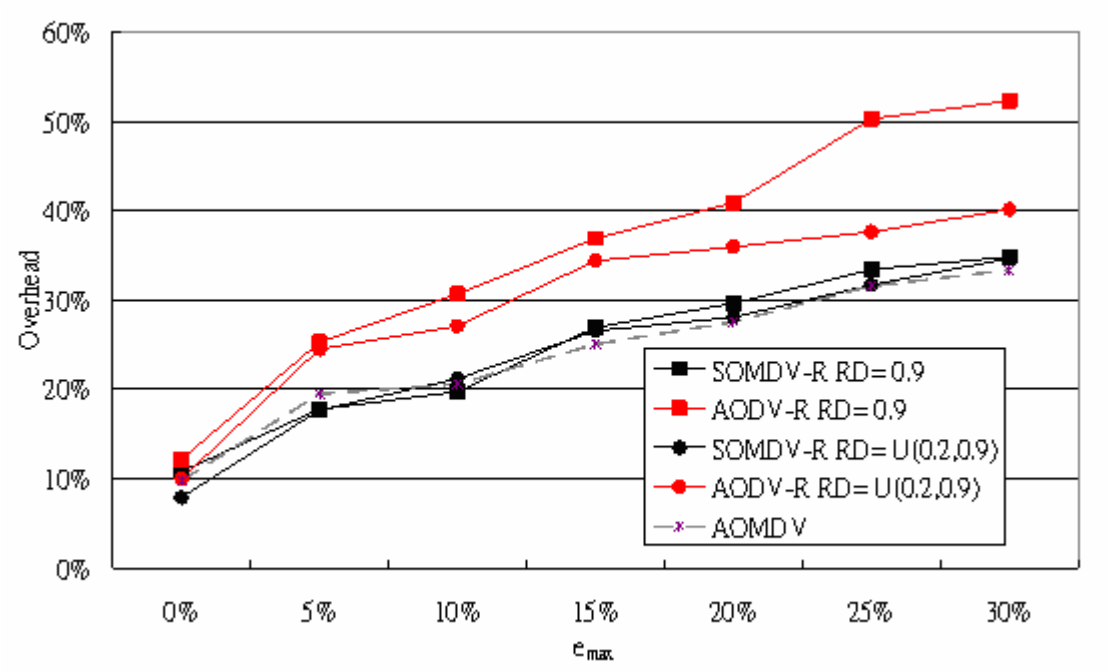


Figure 4-5 Overhead with RD_s = Random (0.2, 0.9) and RD_s = 0.9

In Fig. 4-6, we simulate the overhead under different RD_s and channel error rate. The overhead of high RD_s is 3% more than the low RD_s in average. The slight difference is because the increase of the amount of the control packets maintaining the reliable paths. When RD_s is high, the frequency of route discovery process will increase and thus increase the routing overhead.

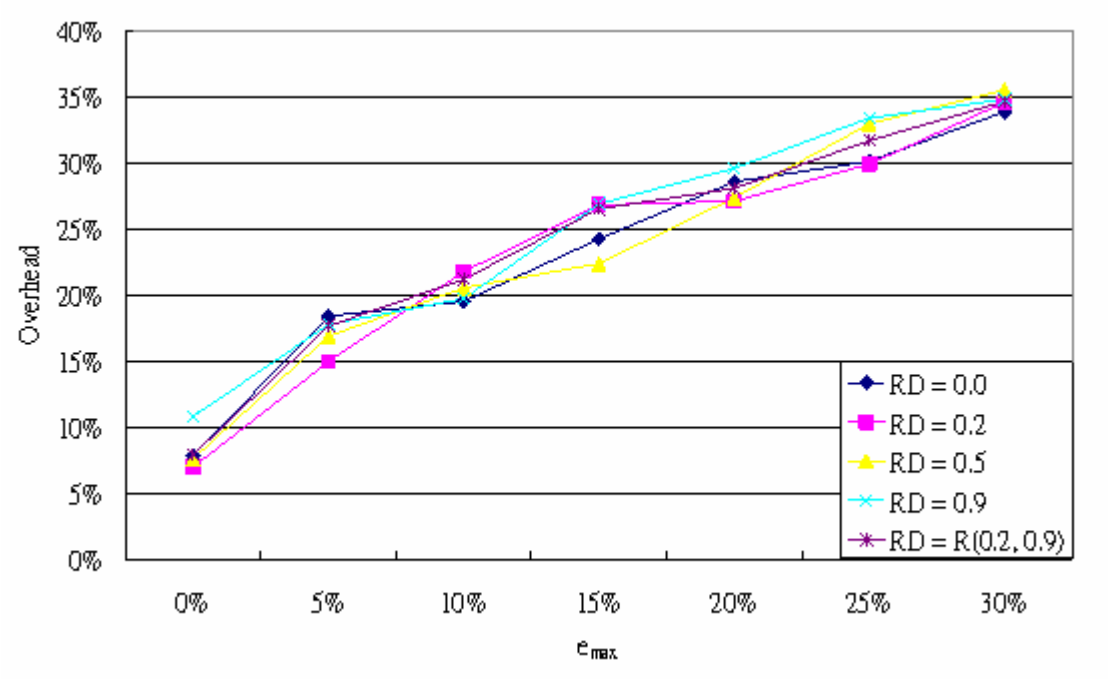


Figure 4-6 Overhead with different RD_s

4.3.3 Latency

Fig. 4-7 shows the mean end-to-end latency for the data packets under different number of connections. The channel error rate is uniformly distributed between 0% and 20%, the reliability demand (RD_s) is randomly choose between 0.1 and 0.9 in SOMDV-R and AODV-R. We compare the mean latency between SOMDV, AOMDV, and AODV-R. These three protocols have almost the same mean latency under light traffic load such as 10 connections. But with the connections increases to 50, the mean latency of AODV-R raise promptly due to the single path maintenance. AODV-R initiates the route discovery process more frequently and the packets will spend more time in being buffered. SOMDV-R has slightly greater mean latency than AOMDV under all number of connections due to the trade-off between reliability and latency. In general, SOMDV is outperformed than AODV-R in reducing 50% of mean latency.

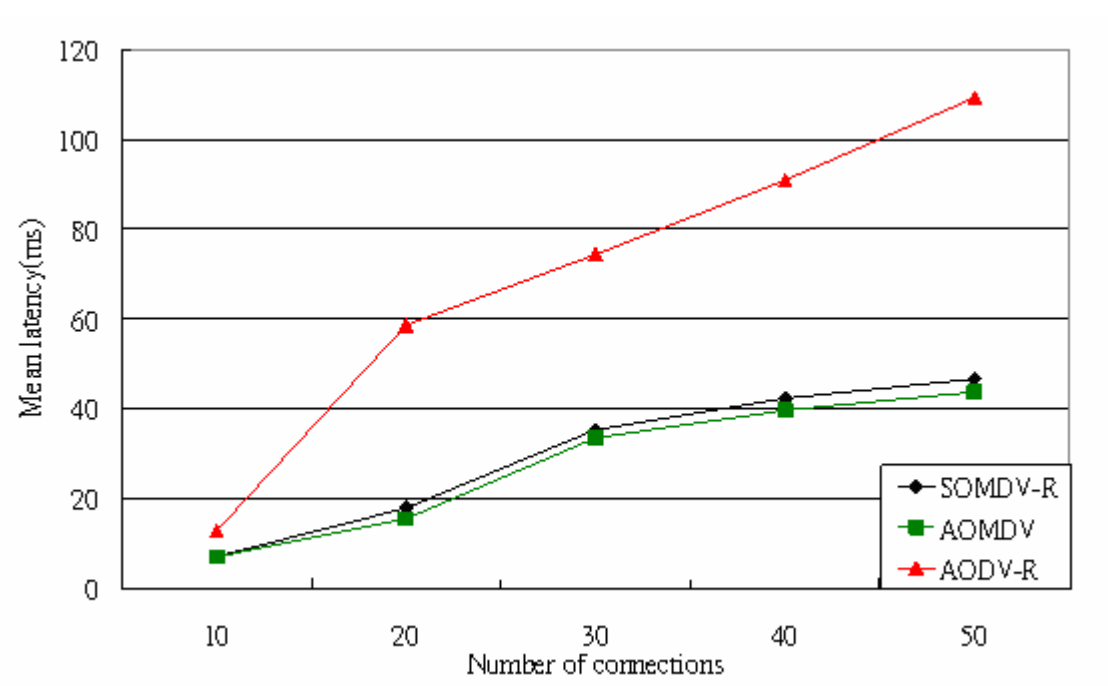


Figure 4-7 Mean latency

4.3.4 Ratio of Forwarding Paths

Fig. 4-8 shows the ratio between the numbers of paths SOMDV-R will use while making forwarding decision. There are 10 CBR connections in the network and the RD_s of each connection is randomly assigned between 0.7 and 0.9, which is a quite high demand. We vary the max channel error rate from 0% to 30% with interval 5%. From the Fig. 4-10, the number of using single path decreases with the raising of the channel error which means single path is insufficient under high channel error rate. The curve of "Two Paths" stops increasing until the channel error exceeding 15%. This implies that if the channel error rate is low, SOMDV-R is able to satisfy the reliability demand by using two paths; if the RD_s is quite high, the chance of using two paths to achieve the reliability demand is no longer easy. The only solution is to use more paths simultaneously to overcome the poor channel condition and satisfy high reliability demand.

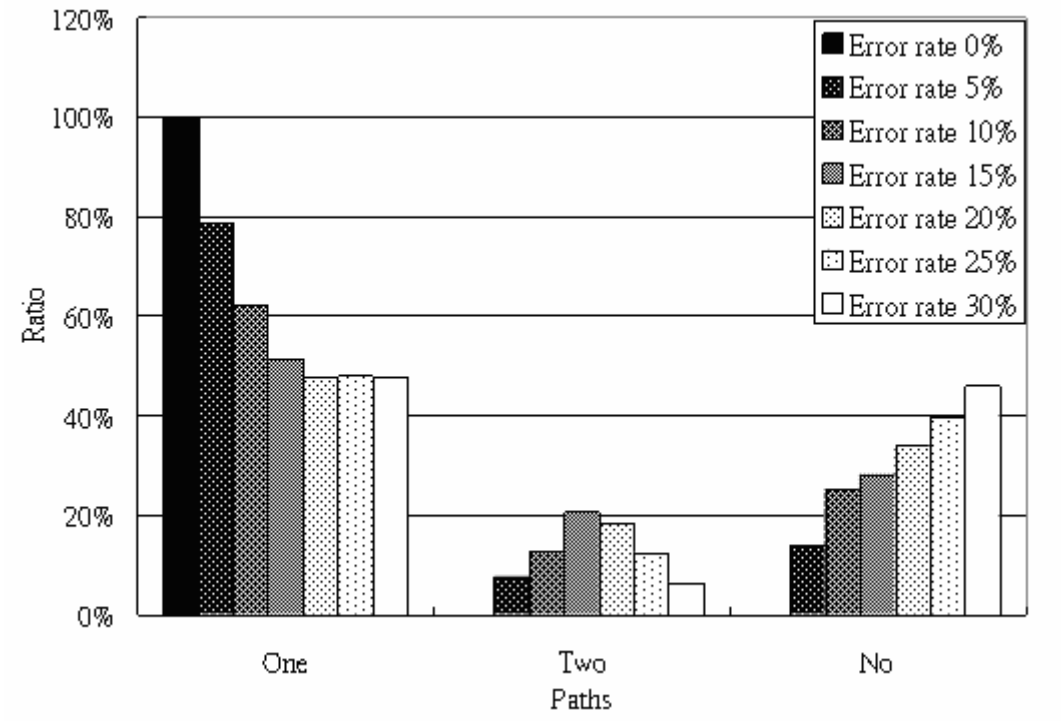


Figure 4-8 Ratio between different number of paths

Chapter 5.
Conclusions and Future Work

Wireless sensor networks are composed of many sensor nodes with power supplied by batteries and a sink node which is connected to the Internet or an information gathering system. Every scheme developed for WSNs should consider both energy-efficiency and low overhead since the resource is limited. The main function of WSNs is to sense the event and report it to the sink. Designing a routing protocol with energy-efficiency or minimum overhead is insufficient for some applications which are aim to provide reliability to the data. Those applications include fire alarm detection, security usage for a bank or an office…etc. The generating data will have different reliability demands so the routing protocol must offer different reliable paths for these packets.

In the thesis, we propose a reliable routing protocol for WSNs which can provide reliability to the packets and maintain minimum routing overhead called SOMDV-R. SOMDV-R is a reactive, fully distributed, and multiple paths routing protocol designed for wireless sensor networks. It greatly reduces the routing overhead by maintaining multiple paths to the sink in each route discovery process. With different data forwarding mechanism, SOMDV-R can forward the data packet according to its reliability demand. From the simulation result, the packet delivery ratio of SOMDV-R is better than AODV-R under different channel error rates and reliability demands due to the multiple paths maintenance. The overhead of SOMDV-R is almost the same with AOMDV since the PE value is piggybacked in the original control packet header, and SOMDV-R does not require any extra type of packet to handle the route management. Comparing to AODV-R, SOMDV-R has smaller routing overhead and

thus can prolong the lifetime of the network. The end-to-end mean latency of SOMDV-R is slightly bigger than AOMDV. In order to provide reliable paths and increase the packet delivery rate, the extra delay caused by buffering packets is necessary.

In this thesis, we assume the sensor nodes are static which is impossible in some applications such as car detection, wild animal observation…etc. In the future, we will simulate the SOMDV-R under dynamic topology. Link quality is changing all the time, thus we have to design a link quality report mechanism which is able to estimate the path in a more accurate way. This mechanism should be considered carefully since the link quality information would be flooded throughout the network. In the simulation, we define the Max_Paths for data packet forwarding as two which is a conservative value for WSNs. This bounded value would influence the packet delivery ratio when the channel error rate is high. As the channel error rate is high such as 30%, the cost for delivering packets with high *RD* would be considerable. The better solution is to use more multiple paths to deliver the packet which will also result in more overhead. This is not expected in wireless sensor networks. Deciding a proper MAX_Paths for WSNs is another issue for future work.

Reference:

[1] D. Ganesan, R. Govindan, S. Shenker, D. Estrin, **"**Highly-Resilient, Energy-Efficient Multipath Routing in Wireless Sensor Networks", *ACM SIGMOBILE Mobile Computing and Communications Conferences*, Vol. 5, Issue 4, Pages11–25, Oct. 2001.

[2] R. Rugin, G. Mazzini, "A Simple and Efficient MAC-Routing Integrated Algorithm for Sensor Network", *IEEE International Conference on Communications*, Vol. 6, Pages 20–24, June 2004.

[3] D. Titan, N. D. Georganas, "Energy Efficient Routing with Guaranteed Delivery in Wireless Sensor Networks", *IEEE Wireless Communications and Networking Conference (WCNC)*, Vol. 3, Pages 1923–1929, Mar. 2003.

[4] H. Cheng, X. Jia, "An Energy Efficient Routing Algorithm for Wireless Sensor Networks", *IEEE Wireless Communications, Networking and Mobile Computing Conference*, Vol. 2, Pages 905–910, Sept. 2005.

[5] H. O. Tan, I. Ko¨rpeog˘lu, "Power Efficient Data Gathering and Aggregation in Wireless Sensor Networks", *ACM SIGMOD Record*, Vol. 32, Pages 66-71, Dec. 2003.

[6] B. Deb, S. Bhatnagar, B. Nath, "ReInForM: Reliable Information Forwarding using Multiple Paths in Sensor Networks", *IEEE Local Computer Networks Conference (LCN)*, Pages 406 – 415, Oct. 2003.

[7] O. Gnawali, M. Yarvis, J. Heidemann, R. Govindan, "Interaction of

Retransmission, Blacklisting, and Routing Metrics for Reliability in Sensor Network Routing", *IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON)*, Pages 34 – 43, Oct. 2004.

[8] S. Dulman, T. Nieberg, J. Wu, P. Havinga, "Trade-Off between Traffic Overhead and Reliability in Multipath Routing for Wireless Sensor Networks", *IEEE Wireless Communications and Networking Conference (WCNC)*, Vol. 3, Pages 1918 – 1922, Mar. 2003

[9] P.K.K. Loh, S.H. Long, Y. Pan, "An Efficient and Reliable Routing Protocol for Wireless Sensor Networks", *IEEE International Symposium on World of Wireless Mobile and Multimedia Networks (WoWMoM)*, Pages 512 – 516, Jun. 2005.

[10] M. K. Marina, R. Das, "On-demand multipath distance vector routing in ad hoc networks", IEEE international conference on Networking Protocols", Pages 14 – 23, Nov. 2001. ; Technical Report Version, "Ad hoc On-demand Multipath Distance Vector (AOMDV) Routing", Apr. 2003.

[11] C. Perkins, E. Belding-Royer, S. Barbara, S. Das, "Ad hoc On-demand Distance Vector Routing (AODV)", *Network Working Group Request For Comments 3561*, Jul. 2003.

[12] Y. Wei, J. Heidemann, D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks", *IEEE/ACM Transactions on Networking*, Vol.12, Issue 3, Pages 493 – 506, Jun. 2004.

[13] J. N. AL-Karaki, A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", *IEEE Wireless Communications Conference*, Vol. 11,

Issue 6, Pages 6- 28, Dec. 2004.

[14] K. Fall, K. Varadhan (Eds). The ns Manual.

http://www.isi.edu/nsnam/ns/doc/index.html , 2006

[15] Stefano Basagni, Alessio Carosi, and Chiara Petrioli, “Sensor-DMAC: Dynamic Topology Control for Wireless Sensor Networks” *IEEE Vehicular Technology Conference*, Vol. 4. Pages 2930 – 2935, Sept. 2004.

[16] Jilei Liu and Baochun Li, “Distributed Topology Control in Wireless Sensor Networks with Asymmetric Links”, *IEEE Global Telecommunications Conference* (GLOBECOM) Vol. 3, Pages 1257 – 1262, Dec. 2003.

[17] Yong Chen and Son, S.H., ” A fault tolerant topology control in wireless sensor networks” Computer Systems and Applications, 2005. *The 3rd ACS/IEEE International Conference*, Pages 57, 2005.

[18] Xiaofei Wang and Toby Berger, “Topology Control, Resources Allocation and Routing in Wireless Sensor Networks”, *Modeling, Analysis, and Simulation of Computer and Telecommunications Systems (MASCOTS) Proceedings*, Pages391 – 399, Oct. 2004.