EMPIRICAL EXAMINATION OF MOBILE AD HOC ROUTING PROTOCOLS ON WIRELESS SENSOR NETWORKS

Zhongwei Zhang[1] and Hong Zhou[2]

[1]Department of Mathematics and Computing, University of Southern Queensland, Toowoomba, QLD 4350
zhongwei@usq.edu.au
[2] Department of Electronic Engineering, University of Southern Queensland, Toowoomba, QLD 4350
hzhou@usq.edu.au

ABSTRACT

Wireless sensor networks (WSNs) have great potential of being deployed in many places where traditional wired or wireless networks are not feasible. But they have also many new challenges more than other wireless networks. These challenges include the design of embedded intelligent sensors and wireless networking technology, ie. routing protocols and network security. WSNs also have some constraints such as sensor nodes failure which render WSN unavailable. The routing protocol in the sensor networks plays a critical role. They influence the performance of the WSNs and have significant impact on the security and the availability of WSNs. Wireless sensor networks (WSNs) have been regarded as an incarnation of Ad Hoc Networks for a specific application. Since a WSN consists of potentially hundreds of low cost, small size and battery powered sensor nodes, it has more potentials than a MANET to be deployed in many emerging areas. However, they also raised many new challenges, and these challenges include the design of embedded sensors and wireless networking technology, ie. routing protocols and network security.

Many ad hoc routing protocols such as AODV, DSR, DSDR, TORA and OLSR, which have been developed particularly for the mobile wireless ad hoc networks (MANETs), performed satisfactorily on MANETs. Research has shown that these ad-hoc routing protocols work well for MANETs with different characteristics and requirements. In this paper, we investigate how well these ad-hoc routing protocols work on wireless sensor networks (WSNs). We focus on their performances in terms of average end-to-end delay, packet delivery ratio and routing overheads.

KEYWORDS

Wireless technology, Sensor nodes, Dynamic routing, Throughput, Wireless Network, End-to-End delay

1. INTRODUCTION

Ubiquitous and Pervasive Computing deal with providing users with computing and communication services all the time and everywhere [6]. Recent advances in sensing electronics and wireless communication technology have enabled a group of sensors to sense the surroundings and communicate with each other without a fixed infrastructure. A communication network of such a kind is called a wireless Ad Hoc networks (MANET). As an embodiment of MANET, Wireless sensor networks are the first step of pervasive computing towards the practical application of wireless Ad hoc networks [4].

Wireless sensor networks have a rigorous requirement for routing protocols. WSNs often integrate a wired network and a wireless network consisting of hundreds of sensor devices. The sensor devices are powered by batteries which likely are irreplaceable. The sensing data will be forwarded to a gateway which will communicate with the data process server.

WSNs usually consist of a group of mobile sensor nodes and a fixed gateway station. The mobile sensor nodes are delivering their sensed data to the gateway and they critically rely on the routing protocols to identify the optimal route at that particular time. That indicates the routes changes over time due to the movement of sensor nodes, or some sensor nodes running out of energy.

Due to their attractive characteristics, WSNs can be deployed in many environments for different purposes [1]. The scope of deployment which has been growing in the last few decades, covers many areas such as disaster management, border protection and combat field surveillance. Basically WSNs have the potential of being deployed any place where humans can not easily access or there is danger to human life.

Ad hoc routing protocols such as ADOV, DSR, DSDV and OLSR have been investigated on the MANETs in the past few years. The investigation of the performance of these protocols on the MANETs has produced many useful results. However, we have seen very limited findings of how these ad-hoc routing protocols perform on wireless sensor networks [5, 10]. Nonetheless, we can see many attempts at developing routing protocols for WSNs under the different deployment of WSNs [7].

The objective of this research is to develop an optimal routing protocol for practical wireless sensor networks. The second objective of this research is to deal with the problem of the security of sensor networks at routing level. The optimal routing protocol for sensor networks means a routing protocol can use the sensor energy most efficiently.

This paper is structured into six sections. We start with looking at the performance of WSNs in Section 2 and how the routing affects security and connectivity. In Section 3, we illustrate various routing protocols in use today. In Section 4, we will run a number of experiments on NS2 which will use the routing protocols reviewed in Section 3. Section 5 is dedicated to an experimental comparison of these routing protocols under a number of scenarios. Finally we conclude the paper in Section 6 by summarising the results and listing out a few possible research topics for the future.

2. WSN PERFORMANCE AND SECURITY

Without a fixed structure, mobile nodes in WSNs include sensor nodes and phenomena nodes. Figure 1 shows a sketch of a wireless sensor network, where a sensor node moves around the physical environment. Once a sensor node detects a target, it generates a data packet and sends it to the sink node via the wireless channel. The sink node collects all data packets from sensor nodes, and sends them to the user. WSNs can be evaluated in terms of availability, reliability, response time, utilisation, throughput, bandwidth capacity, and packet loss ratio [9]. WSNs' performance is largely dependent on the design of WSNs in which the routing protocols, topology, and energy model are the main factors [3]. In contrast to traditional wired networks with a fixture, the performance of WSNs is closely related to the routing performance due to the fact that the routes are dynamically varying all the time. The routes on the WSNs are

periodically updated according to the mobility of sensor nodes and the fact that some sensor nodes might run out of energy.

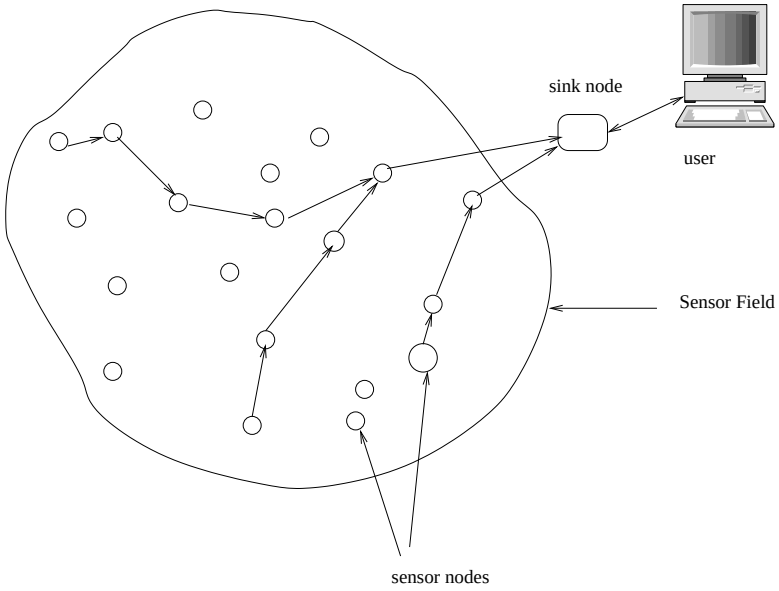

Figure 1: A diagram of a wireless sensor network

The routing performance will impact not only on the security of WSN [2, 8], but also on the connectivity or availability of the WSNs. Within WSNs, the sensor nodes always find a few neighbour nodes to relay the data to the sink nodes. That means the possibility of forming multiple routes is high. As a result, the routing protocol may take security into account when selecting the optimal routes among several possible routes. On the other hand, if the routing protocols also consider the energy level in their neighbour nodes while determining the best route, the protocol may find a route which maximises the lifetime of WSNs, ie. extending the availability of WSN.

In this research, we focus on how routing impacts on performance and security. The routing of the WSNs means how a route is formed once a sensor node wants to send the sensed data to the sink nodes. Due to the mobility of the sensor nodes and the sink nodes, the routing is dynamically changing.

3. AD HOC ROUTING PROTOCOLS OVERVIEW

In this section, we briefly review five of the most used Ad Hoc routing protocols. Ad Hoc Routing protocols can be categorised into three classes: proactive, reactive and a bit of both (hybrid) by looking at their nature. That means if a sender will actively find a route to the intended receiver whenever the sensor needs to send a message to the receiver, the protocol used is classed as proactive. For example, among ad hoc network routing protocols, AODV and DSDV are proactive while TORA and DSDV are reactive. OLSR is a bit of both. Following is how each of five ad-hoc routing protocols all used in MANETs: AODV, DSDV, DSR, TORA and OLSR works.

3.1. DSDV: Destination-Sequenced Distance-Vector routing

DSDV is based on the idea of the classical Bellman-Ford routing algorithm with some improvements. DSDV is a proactive, distance vector protocol. Each node maintains a routing table that lists all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination node. The nodes periodically transmit their routing tables to their immediate neighbours. A node also transmits its routing table if a significant change has occurred in its table from the last update sent.

3.2. DSR: Dynamic Source Routing

DSR is a reactive routing protocol. This protocol works as follows: Each node can discover dynamically a source route to any destination in the network over multiple hops. A complete, ordered list of the nodes through which the packet must pass is included in each packet header. Main mechanisms of DSR include **Route Discovery** and **Route Maintenance**. These two mechanisms work together to discover and/or maintain source routes to any destination in the networks.

3.3. AODV: Ad Hoc On-Demanding Distance Vector routing

AODV combines the mechanisms of DSR and DSDV. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. An important feature of AODV is the maintenance of timer-based states in each node, regarding utilisation of individual routing table entries.

AODV uses a destination sequence number for each route entry. The destination sequence number can be used to ensure loop-free and to identify which route is newer. The principle AODV uses to choose the route among multiple routes is to select the one with the greatest sequence number.

3.4. TORA: Temporally Ordered Routing Algorithm

TORA is a distributed routing protocol based on a ``link reversal'' algorithm. It discovers routes on demand. It provides multiple routes to a destination, establishes routes quickly, and minimises communication overhead by localising algorithmic reactions to topological changes when possible.

3.5. OLSR: Optimised Link-State Routing

OLSR is a proactive link-state routing protocol. It uses periodic messages for updating the topology information.

OLSR is based on the following mechanisms:

- neighbour-sensing based on periodic exchange of HELLO messages
- efficient flooding of control traffic using the concept of multiple relays
- computation of an optimal route using the shortest-path algorithm.

4. EXPERIMENT ON NS2

In this section, we experiment with these routing protocols using simulation technology. In our experiments, all sensor nodes are set up with a high energy level. The starting level of sensor nodes is $2.5J$.

Energy management is one of the major factors that influence the performance of WSNs. Here the performance metrics of WSNs is an issue. For instance, let's talk about the routing overhead. Our objective is to evaluate the routing protocol on a WSN with different scenarios. We achieve this objective by finding out and then comparing three performance indicators as follows.

- **Packet delivery fraction** The ration of the data packets delivered to the destinations to those generated by the CBR sources

- **Average end-to-end delay of data packets** This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.

- **Normalised routing load** The number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission.

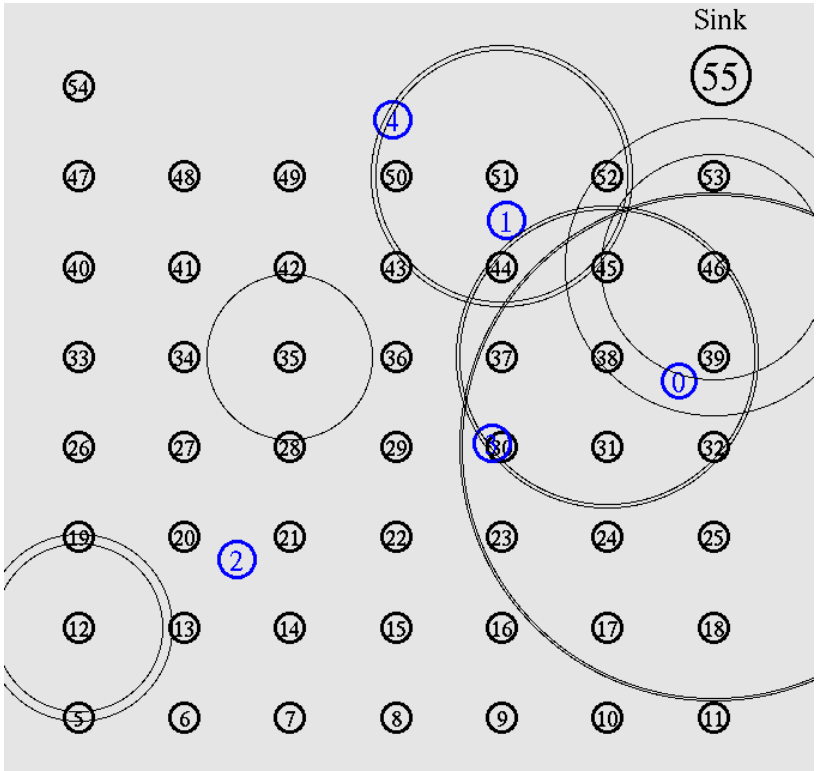

Figure 2 A Wireless sensor network

Figure 2 shows a wireless sensor network where the nodes in blue are the phenomena nodes and other nodes are the sensor nodes. The phenomena nodes emit a signal and the sensor nodes

surrounding it will sense the phenomenon and then send the signal to the gateway node or a sink node (ie. node 55).

4.1. NS2 Network Simulator

The NS2 simulation environment used by many researchers features as a flexible tool for networking researchers to investigate how various routing protocols perform with different network configurations and topologies. NS2 can be used as a platform to design new routing protocols. In the past few years, many extensions to NS2 have been developed for wireless networks and wired-cum-wireless networks. We use the network simulator NS2 and the NRLsensim extension [5]. We have set up our experiment as in Table 1.

Table 1: Parameters used in NS2 simulation

Simulation time	900 seconds(15 minutes)
Number of mobile nodes	50
Max speed of mobile node	20 m/s
Area size	1500m x 3000m
MAC	IEEE 802.11
Propagation mode	Two ray ground
Node mobility	Random
Traffic	Constant bit rate (CBR)
Agent	UDP
Queue length	50 bytes
Number of sources	1, 3, 5, 7
Pause time	0s, 10s, 20s, 30s, 40s, 50s

The source nodes are the sensor nodes that have detected a phenomenon and need to transmit the sensed data to the sink node (ie. the gateway node). The source nodes follow a Gaussian distribution. The pause time is the time that a sensor node takes between two movements.

4.2. Performance of WSNs using AODV

Figure 3 shows how AODV performs under the WSNs.

We can see that the average end-to-end delay of the packet transmission is between 10 to 100 with just one source. The more sources there are, the higher the end-to-end delay. The routing overheads involved are much more for multiple sources than the single source WSN. Note that the routing overhead for the WSNs with 7 sources is a little bit strange. The packet delivery ratio is above 40% for all multiple sources, it is worth pointing out that the packet delivery ratio is always above 90% for the single source.

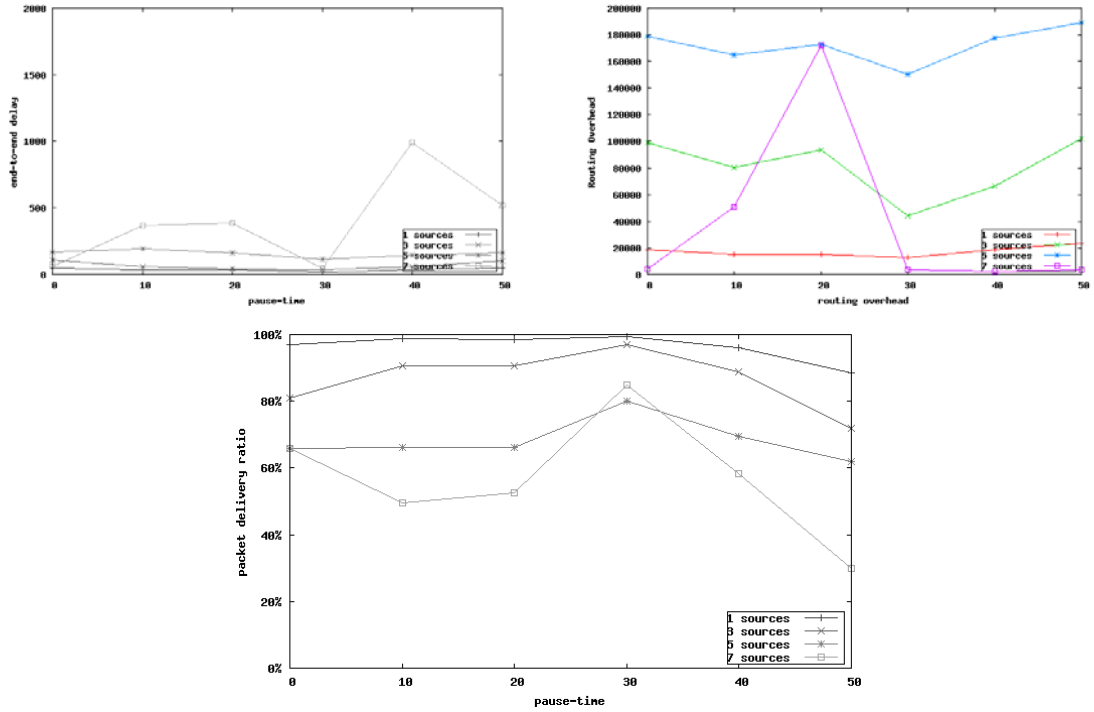

Figure 3: AODV on WSN

4.3. WSNs using DSDV

Figure 4 depicts the performance of the DSDV on WSNs with 50 nodes.

The end-to-end delays involved in each of WSNs are all within the 0 to 1000ms band. The more sources there are, the large the delay. This is very easy to understand. Similarly the routing overheads are slightly varying for all the pause times. This indicates the DSDV performs very stable on WSNs with one or multiple sources all the time. Of course, the more sources in it, the higher the routing overheads involved. Interestingly, the packet delivery ratios are all within 40% to 80%. This is a very good result. This is the best performance a protocol performed on WSNs we have seen so far.

If there is one source, the end-to-end delay is between 0 and 500*ms* which is not that bad, but the end-to-end delay for multiple sources are ridiculous too high, therefore DSR is not workable, although the routing overheads and the packet delivery ratio are reasonable.

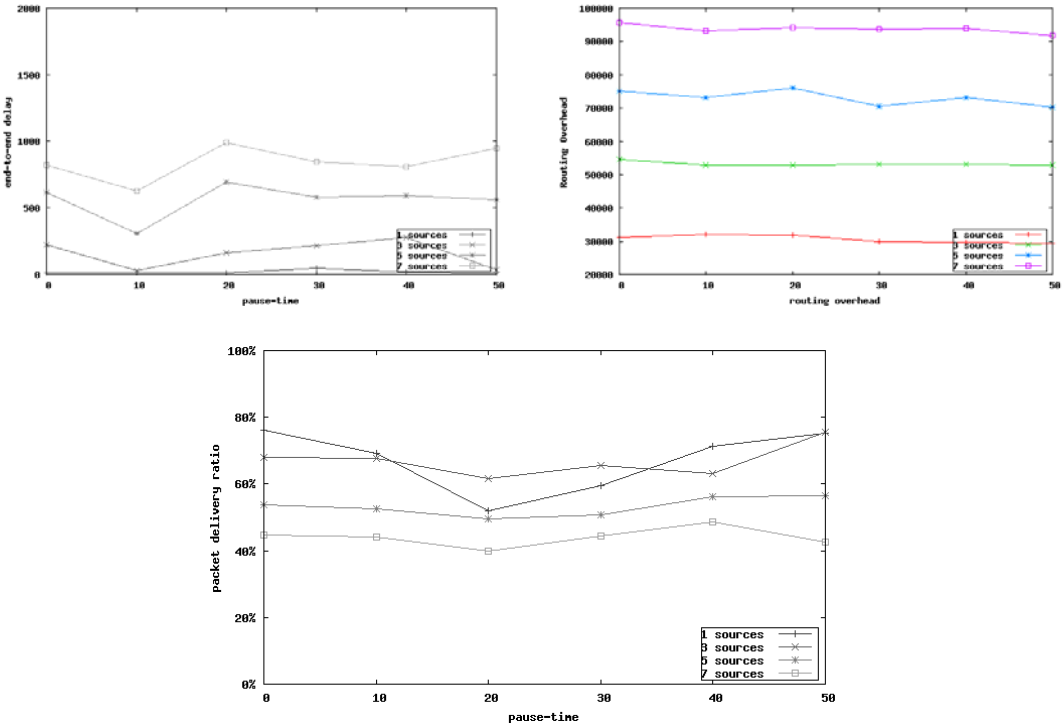

Figure 4: DSDV on WSN

4.4. Performance of WSNs using DSR

Figure 5 shows how the DSR performs on the WSN.

4.5. WSNs using TORA

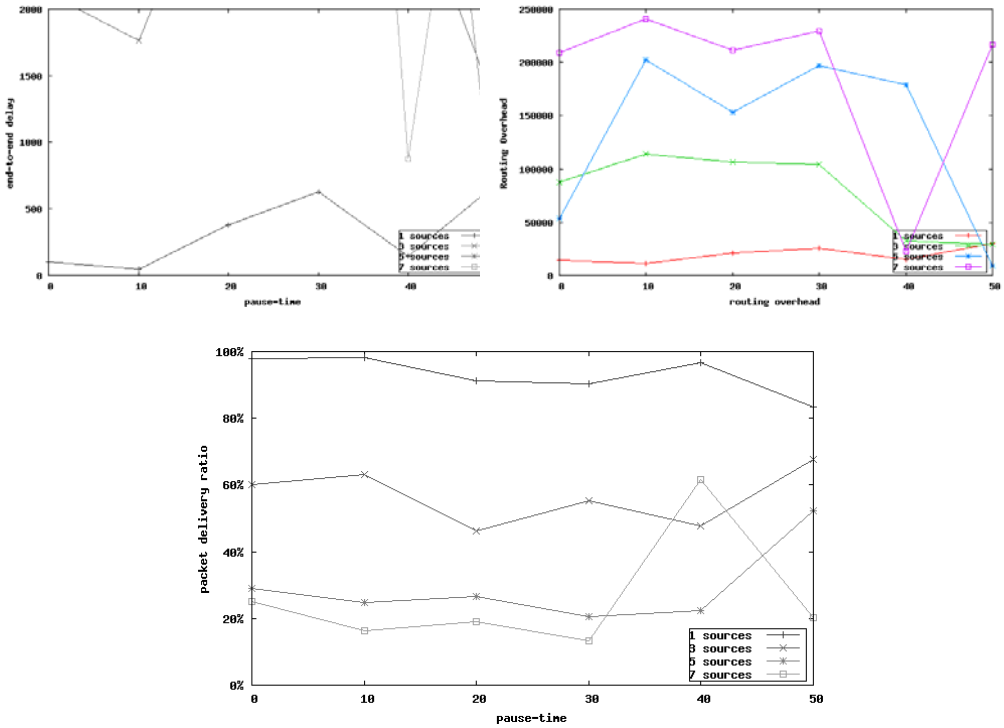

Figure 5: DSR on WSN

TORA performs on WSNs in a quite abnormal manner, as shown in Figure 6.

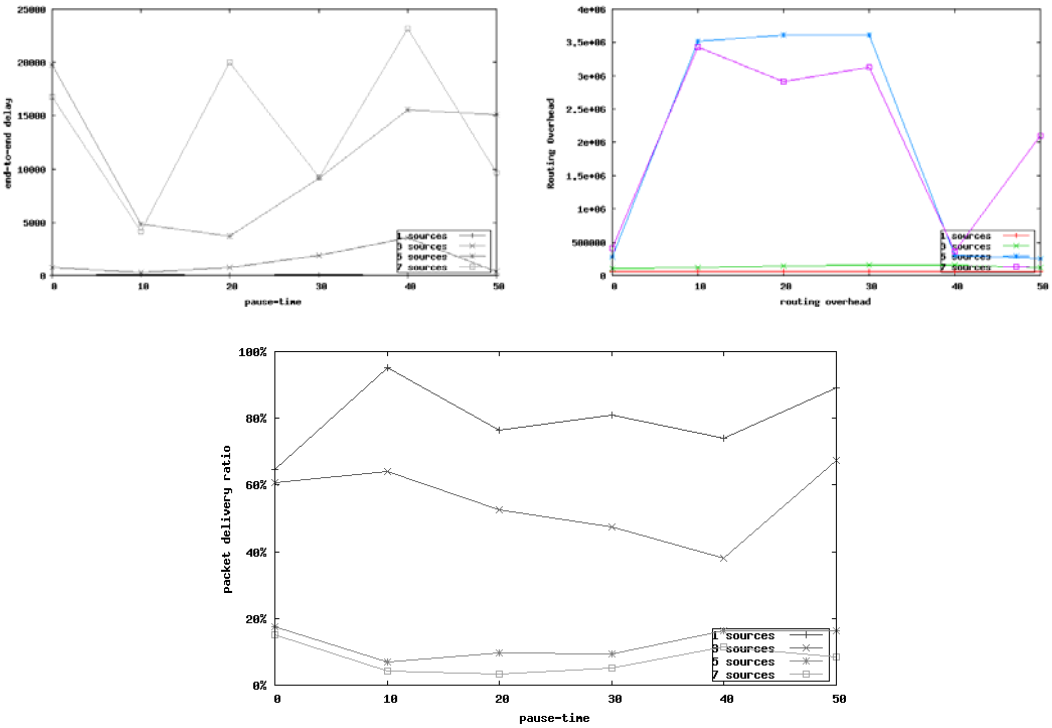

Figure 6: TORA on WSN

If there are one or two sources in WSNs, the end-to-end delays are acceptable, and the routing overheads are also pretty low. The packet delivery ratio can reach as high as 80%. However, if there are more than two sources, TORA becomes unusable. That means the end-to-end delays are unacceptably high, as are the routing overheads. Consequently the packet delivery ratio drops to as low as 10% or even less.

4.6 WSNs using OLSR

Figure 7 shows the performance of OLSR on WSNs. Comparing Figure 7 with Figure 6 we can see that OLSR has a reasonably good end-to-end delay time for up to three sources. They are all below 200*ms*. The routing overheads are relatively stable for the WSNs with one source and three sources. But the routing overheads for the WSNs with three and seven sources are acceptable and the overhead for the WSNs with one source is too high. Interestingly, the packet delivery ratios for all the WSNs are between 40% and 80%, which are pretty good in principle.

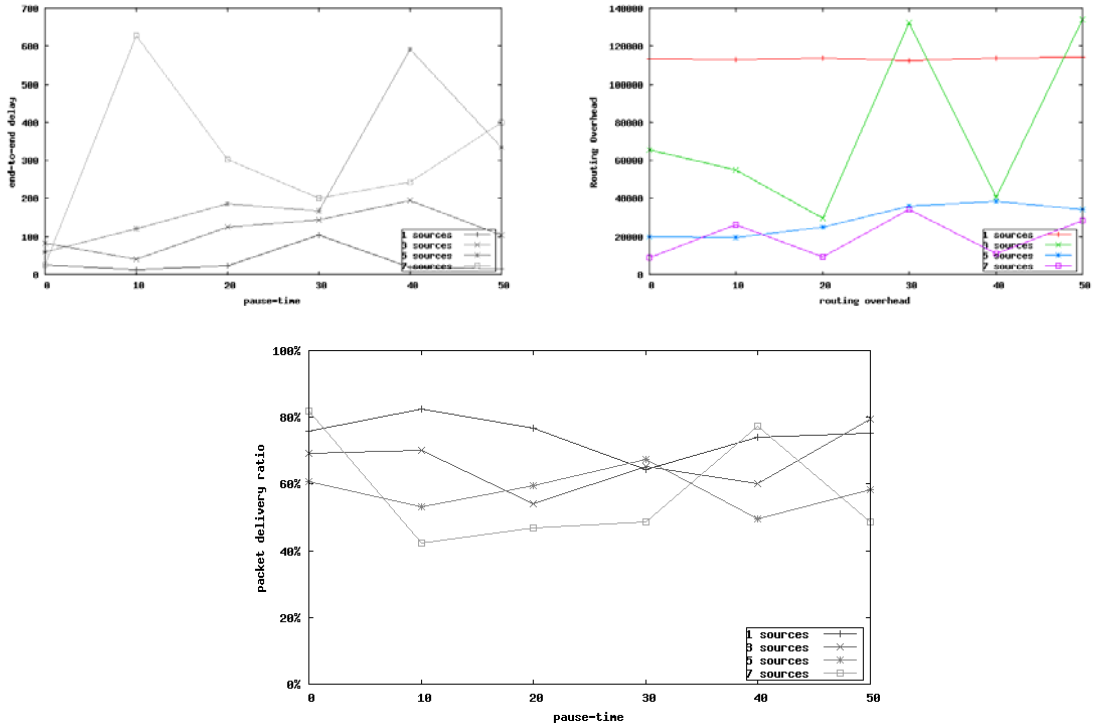

Figure 7: OLSR on WSN

5. PERFORMANCE COMPARISON

In this section, we compare various performances in terms of packet delivery fraction, average end-to-end delay of data packets and normalised routing load. The packets which have been sent can be counted at all levels, including the application level and router and MAC level. We think it would be fair to count the sent packets in the MAC. Another point is that the packets which have been forwarded should be counted as well. Therefore, either the routing packet or data packet should be the MAC packets which have been either sent or forwarded.

5.1. WSNs with one source

In Figure 8, we show different performances on the WSNs with one source. AODV, DSR, DSDV and OLSR have acceptable routing overhead, the routing overheads occurring in TORA is a bit too high. The packet delivery ratios are all above 60%, although DSDV performing on WSNs has a relatively low packet delivery ratio.

5.2. WSNs with three sources

On the WSNs with three sources, the performance of these routing protocols has a a little change, as shown in Figure 9. From Figure 9, we can see that both TORA and DSR have high routing overheads, but DSDR and OLSR perform in almost the same way. It is worth noting that DSDV always has a stable routing overhead, but OLSR has improved. However, most of the routing protocols have a worse packet delivery ratio. That is, all except AODV have dropped their packet delivery ratio to around 60%.

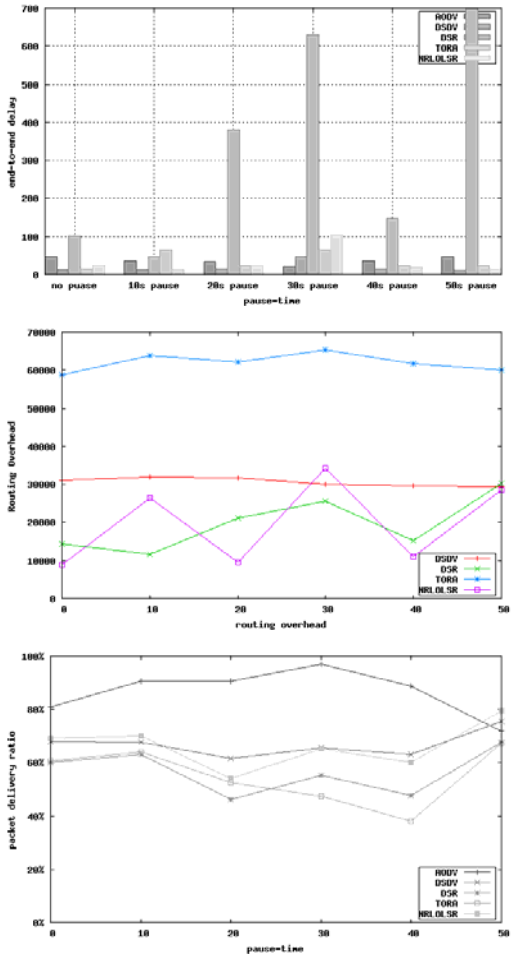

Figure 8: Performance comparison with 1 source

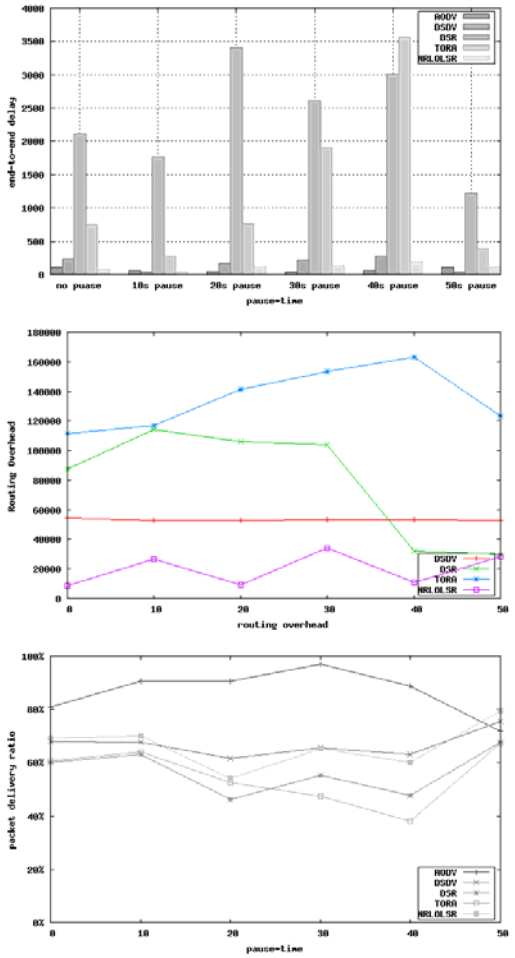

Figure 9: Performance comparison with 1 source

5.3. WSNs with five sources

As we can see in Figure 10, TORA requires prohibitively high routing overheads when these protocols work on the WSNs with seven sources, although others remain the same as on the WSNs with one and three sources. The packet delivery ratio of these routing protocols has been significantly affected. Note that all the routing protocols except AODV have dropped their packet delivery ratio below 60%.

5.4. WSNs with seven sources

Very similar to the WSNs with five sources, the routing overheads and packet delivery ratio of these routing protocols on the WSNs with seven sources are shown Figure 11. The overall results slightly worsen, although the overall trend remains the same.

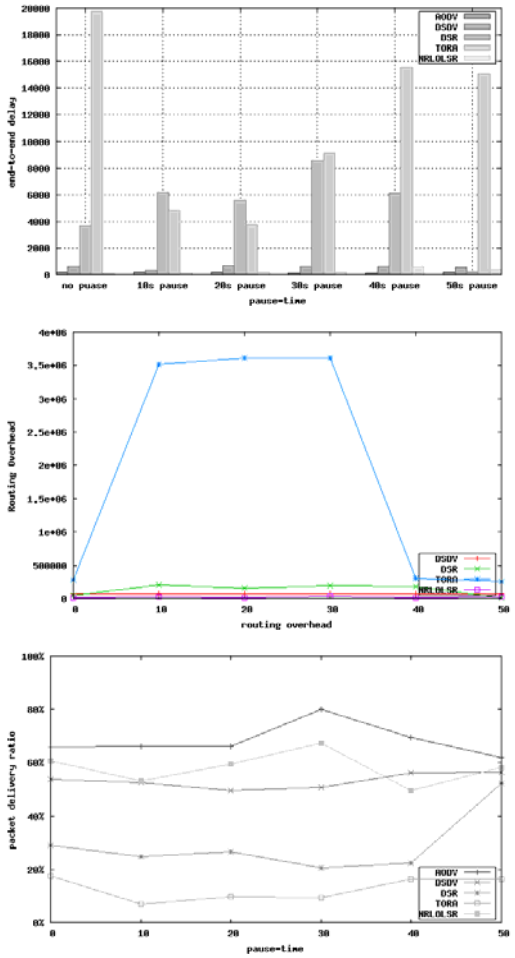

Figure 10:Performance comparison with 5 sources

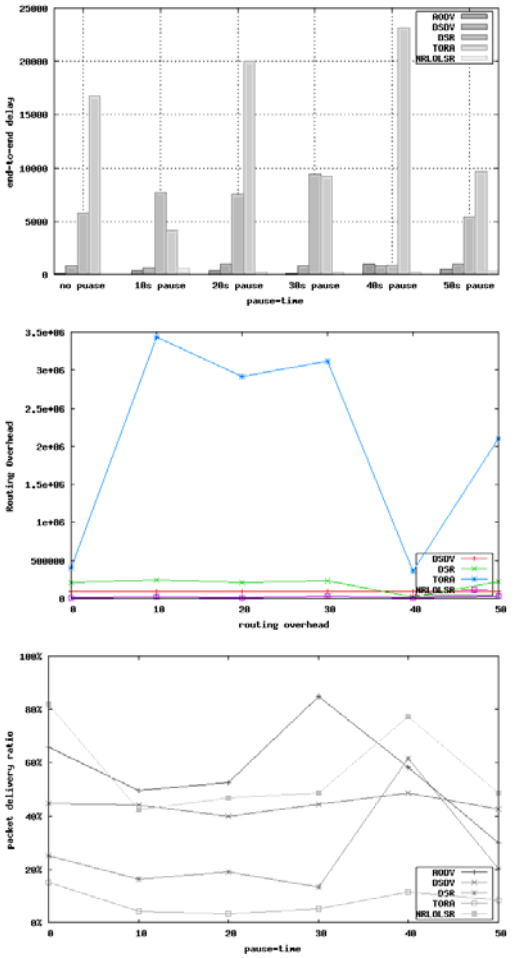

Figure 11: Performance comparison with 7 sources

6. CONCLUSIONS

In this paper, we have reported possible application areas of wireless sensor networks. We also pinpoint the challenges of the current WSNs, mainly in the routing protocols. An illustration of the routing protocols has been given.

As expected, the routing protocol, which WSNs have adopted from the Ad Hoc routing protocols, have influenced the performance of WSNs. We have studied AODV, DSR, DSDV, TORA and OLSR on the WSNs and discussed their performance in terms of the average end-to-end delay, packet delivery ratio and the routing overhead on a WSN with a different number of sources. For each individual routing protocol, there are some merits and drawbacks shown under different scenarios. For instance, we have demonstrated that the TORA on WSNs having multiple sources has a too high average end-to-end delay, which is unacceptable. Comparing all these routing protocols under the same WSNs with the same scenarios, we found that AODV always performs better on all WSNs with single or multiple sources. DSDV is next to the AODV despite DSDV has a relatively low packet delivery ratio.

Our findings seem to suggest that if we intend to extend the ad hoc routing protocol with the security level and energy efficiency for the WSNs, DSDV and AODV are two candidates. These two protocols have a routing table in their nodes, and the optimal route will be calculated within each sensor nodes. It is advisable to add security level and energy level into the routing algorithm in the future.

REFERENCES

[1] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and E. Cayirci (2002). *A survey on sensor networks*. IEEE Communications Magazine, Aug 2002. pp 102-114.

[2] H. Chan and A. Perrig, (2003) *Security and privacy in sensor networks*. IEEE Computer, Oct 2003. pp 103-105.

[3] Carla Fabiana Chiasserini and Michele Garetto, (2004) *Modeling the performance of wireless sensor networks*. IEEE INFOCOM, Hong Kong, March 7-11, 2004.

[4] Marco Conti and Silvia Giordano, (2007) *Multihop Ad Hoc Networking: The Reality*, IEEE Communication Magazine, April 2007. pp 88-95.

[5] Ian Downard, (2004) *Simulating sensor network in ns-2*. NRL Formal Report 5522.

[6] Deborah Estrin, David Cullar, Kris Pister and Gaurav Sukhatme, (2002) *Connecting the Physical World with Pervasive Networks*, Pervasive Computing, Jan 2002. pp 59-69.

[7] Qiangfeng Jiang and D. Manivannan, (2004) *Routing Protocols for Sensor Networks*, Consumer Communications and Networking Conference, First IEEE Volume Issue, Jan 2004. pp 93-98.

[8] Anthony D. Wood and John A. Stankovic (2002) *Denial of Service in Sensor Networks*, IEEE Computer, Oct 2002. pp54-62.

[9] Yunjiao Xue, Ho Sung Lee, Ming Yang, Priantha Kumarawadu, Hamada H. Ghenniwa and Weiming Shen (2007) *Performance Evaluation of NS2 Simulator for Wireless Sensor Networks*, IEEE, 2007. pp 1372-1375.

[10] H. Zhou, J. Lu, Z. Zhang, H. Ali, and C. Won (2007) *Application and performance of extended TTDD's in large-scale wireless sensor networks*. MSN 2007, LNVC 4864, Dec. 2007. pp 135-142.

Authors

Zhongwei Zhang(S'97-M'00) received the B.Sc degree in Applied Mathematics from Harbin Institute of Technology, China, in 1986, the Masters degree of Computer Science from the University of Amsterdam, the Netherlands 1992, and the Ph.D degree in computing from Monash University, Victoria, Australia in 1998.

He has been a Senior lecturer at the University of Southern Queensland, Australia since 2003. In 2003, he was a visiting professor at the University of North Carolina at Greensboro, USA. His current research include wireless communication networks, routing and security on wireless sensor network, modelling and optimisation in TCP/IP networks, network security, information fusion techniques, and E-Commerce technology.

Hong Zhou received B.Sc degree in Engineering (with University Excellent Graduate Award) from Liaoning Technical University, China in 1987, and Masters degree of Engineering from Shenyang Institute of Technology, China in 1990, and the Ph.D degree in 2002 from Curtin University of Technology, Australia.

She has been lecturing at the University of Southern Queensland, Australia since 2003. From 2002 to 2003, she was a Postdoctoral research fellow at University of Technology Sydney. She has been a senior systems engineer at Genista Research Pty.Ltd., Singapore from 2001 to 2002.

Dr Zhou research interests include Wireless sensor networks, wireless communication, computer networks and software engineering. She was a visiting scholar at College of Information Science and Technology, University of Nebraska, Omaha, June-July, 2006.