School of IT
Technical Report

The University of Sydney

A PROCEDURE FOR BENCHMARKING MAC PROTOCOLS USED IN WIRELESS SENSOR NETWORKS

TECHNICAL REPORT 593

DEREK J CORBETT[1], ANTONIO G RUZZELLI[2]
DAVID EVERITT[1] AND GREGORY O'HARE[2]

[1] SCHOOL OF INFORMATION TECHNOLOGIES, THE UNIVERSITY OF SYDNEY
[2] SCHOOL OF COMPUTING AND INFORMATICS, UNIVERSITY COLLEGE DUBLIN

AUGUST, 2006

A procedure for benchmarking MAC protocols used in wireless sensor networks

Derek. J. Corbett[1]*, Antonio. G. Ruzzelli[2,], David. Everitt[1] and Gregory. O'Hare[2]

[1] *School of Information Technologies, The University of Sydney, NSW 2006, Australia.*
[2] *School of Computing and Informatics, University College Dublin, Belfield D4, Dublin, Ireland.*

SUMMARY

The development of new MAC protocols to deal with emerging applications for infrastructure-free networks, such as wireless sensor networks, is currently impeded by the lack of a common benchmarking standard to determine the suitability of certain protocols to certain scenarios. There is a need to rectify this situation to facilitate the development of new MAC protocols by improving the quality of their evaluation. To achieve this goal, the current methods, scenarios and metrics used for evaluating MAC protocols for wireless sensor networks are surveyed, and a common application independent benchmark is formulated to assess the suitability of new and emerging protocols.

KEY WORDS: MAC; Simulation; Wireless Sensor Networks

1. INTRODUCTION

Wireless sensor networks (WSNs) are networks composed of many small, independent, sensor nodes. These nodes are designed to collaborate together in order to sense the environment in which they are deployed. The key difference between sensor networks and other infrastructure-free networks in which inter-node collaboration is necessary, such as MANETs and Ad Hoc Networks, is a more pertinent need for energy efficiency in sensor networks. When a multitude of sensor nodes are placed in their target environment, battery replacement becomes difficult and in some cases impossible. As sensor networks perform their function through inter-node collaboration, the lifetime of the network is highly dependent on the lifetimes of the sensor nodes, which are in turn dependent on the energy efficiency of the protocols deployed on these nodes.

---

*Correspondence to: School of Information Technologies, The University of Sydney, NSW 2006, Australia.

Contract/grant sponsor: Derek J. Corbett and David Everitt acknowledge the continuing support of the Smart Internet Technology CRC

Contract/grant sponsor: Antonio G. Ruzzelli and Gregory O'Hare gratefully acknowledge the support of Science Foundation Ireland under Grant; contract/grant number: 03z/IN.3/1361

A sensor node is essentially required to carry out two tasks: interacting with the environment (sensing or actuating) and communicating (reporting sensed data or forwarding other nodes' data). Of these two tasks it is the communication that consumes the largest fraction of the power during the lifetime of the node. The disparity between the cost of communication and computation is revealed in [1]: it is estimated that 3000 instructions can be executed for the same cost as the transmission of one bit of data over 100m. Thus the development of efficient communication protocols is key to the development of successful and deployable WSNs.

The desire for efficient communications protocols has lead to much interest in developing new energy efficient protocols for use at the MAC layer. No fewer than 12 MAC protocols have been proposed for use in WSNs. The amount of activity in this area is encouraging as it provides an enormous amount of choice for sensor network designers. However the lack of uniformity in the evaluation of these protocols means that the choices made by sensor network designers are ill-informed at best. In order to disambiguate the choice of MAC, we propose a benchmarking process than can be applied consistently to all currently proposed MAC protocols for WSNs as well as all future ones. The aim of this paper is not to compare MAC protocols, on the contrary it is to shed light on the best approaches to evaluating them. In the background section 2 we investigate the methods, metrics and scenarios that have been used to evaluate different MAC protocols for WSNs. In the development section 3 we propose a benchmark. The conclusion section 5 offers some thoughts about the use of this benchmark to other researchers and network designers.

2. BACKGROUND

There have been nearly as many approaches to evaluating MAC protocols for WSNs as there have been protocols proposed. This makes comparison between different papers' evaluations of MAC protocols difficult at best. However the key elements of each of these approaches remain the same. The results presented are generally garnered from *simulation*. Different *physical* and *routing* layer protocols are set for these simulations. The simulations are then conducted with different node placements and configurations, which are referred to as *scenarios*. The execution of these simulations results in data which can then be examined in terms of *metrics*. In this section we survey the simulation environments, the physical and routing layers employed, the scenarios and performance metrics used to evaluate and compare MAC protocols for WSNs.

2.1. Simulation Environments

The two preeminent simulation environments for academic network research are ns-2 [2] and OMNeT++ [3]. Their preeminence is not necessarily based on their ease of use, moreover as freely available open source projects they have become the most widely used simulation platforms as they can both be used and extended without concern for licencing expense. An added bonus is that open source protocols developed by researchers can be added back into the simulation projects and evaluated by other researchers. This is particularly useful for researchers who wish to test the cross layer interaction of different protocols. Table I shows the simulation environments used to evaluate the MAC protocols reviewed in this paper.

Table I. Simulation Environments

MAC Protocol	**Simulation Environment**
BMAC [4]	Mote Testbed [5]
DMAC [6]	ns-2 [2]
EMACs [7]	OMNeT++ [3]
IEEE 802.15.4 [8]	ns-2 [2]
LMAC [9]	OMNeT++ [3]
MERLIN [10]	OMNeT++ [3]
μ-MAC [11]	NS-2 [2]
P-MAC [12]	NS-2 [2]
Sift [13]	ns-2 [2]
SMAC [14]	Mote TestBed [5]
Stem [15]	Parsec [16]
TEEM [17]	Mote Testbed [18]
T-MAC [19]	OMNeT++ [3]
TRAMA [20]	QualNet [21]
WiseMAC [22]	GloMoSim [23]
Z-MAC [24]	NS-2 [2] and Mote Testbed [5]

2.2. Physical Layer

The physical layer plays an extremely important role in determining the performance of a particular MAC protocol. Under simulation there are three broad sets of physical layer parameters that can be controlled: bandwidth, broadcast radius and power model, all of which affect the performance of the upper layers and especially the MAC layer. tables II and III present an overview of the various MAC protocol papers surveyed and the physical layer parameters used in their evaluation. It is obvious that there is quite a large disparity between the models used. Even studies which use the same radio module sometimes use different parameters for that model, as seen in TRAMA [20] and Stem [15]. This can make inter-paper comparison difficult if not impossible. Tables IV and V show the actual physical layer parameters for the different varieties of Mote that are commercially available today [†]. Again there is a discrepancy between the parameters that the manufacturers quote and the parameters that are used in evaluation studies. There are several reasons for this. However the most important is that the rate of development of Mote hardware is quite fast, meaning that the parameters listed in the documentation are quickly outdated.

2.2.1. Bandwidth Varying the bandwidth at the physical layer can have drastic effects for the observed performance of upper layer protocols. For example it is possible to mask the latency a MAC protocol introduces to a network by increasing the physical layer bandwidth. Increasing the total available physical layer bandwidth in a shared bandwidth system such as a wireless network has the overall effect of increasing the number of transmissions (successful

---

[†] This information was taken from the technical data sheets available for the different hardware

Table II. Physical Parameters Used

MAC Protocol	**Specific Radio Model**	**Bandwidth**	**Radius**
BMAC [4]	C1000 [25]	N/A	N/A
DMAC [6]	N/A	100Kbps	250m/550m
EMACs [7]	RFM TR1001	N/A	N/A
IEEE 802.15.4 [26]	IEEE 802.15.4	250Kbps	16m
LMAC [27]	RFM TR1001	N/A	N/A
MERLIN [10]	RFM TR1001	115kbps	N/A
μ-MAC [11]	nRF2401 [28]	up to 20Kbps	N/A
P-MAC [12]	N/A	20Kbps	N/A
Sift [13]	N/A	N/A	N/A
S-MAC [29]	TR3000 [30]	20Kbps	N/A
Stem [15]	TR1000 [30]	2.4Kbps	20m
TEEM [17]	TR3000 [30]	20Kbps	N/A
T-MAC [19]	EYES Mote [31]	115Kbps	N/A
TRAMA [20]	TR1000 [30]	115.2Kbps	100m
WiseMAC [22]	WiseNET [32]	25 Kbps	62m
Z-MAC [24]	C1000 [25]	N/A	N/A

Table III. Physical Power Profiles Used

MAC Protocol	**Transmit**	**Receive**	**Idle**	**Sleep**
BMAC [4]	60mW	45 mW	N/A	90μW
DMAC [6]	0.66W	0.395W	0.35W	0W
EMACs [7]	21mW	14.4mW	14.4mW	15μW
IEEE 802.15.4 [26]	31mW	35mW	31mW	N/A
LMAC [27]	21mW	14.4mW	14.4mW	15μW
MERLIN [33]	21mW	14.4mW	14.4mW	15μW
μ-MAC [11]	10.5mA	18mA	N/A	16μA
P-MAC [12]	0.5W	0.3W	N/A	0.05W
Sift [13]	N/A	N/A	N/A	N/A
S-MAC [29]	24.75mW	13.5mW	13.5mW	15μW
Stem [15]	14.88mW	12.5mW	12.36mW	0.016mW
TEEM [17]	24.75mW	13.5mW	13.5mW	15μW
T-MAC [19]	10mA	4mA	N/A	20μA
TRAMA [20]	24.75mW	13.5mW	N/A	15μW
WiseMAC [22]	27 mW	1.8 mW	N/A	5μW
Z-MAC [24]	60mW	45 mW	N/A	90μW

or otherwise) that can be carried out in a period of time. It is particularly interesting to note the vast discrepancies in the bandwidths used in the evaluation of MAC protocols for WSNs shown in table II.

Table IV. Mote Physical Parameters

Motes	**Model**	**Max Bandwidth**	**Radius**
EYES Mote	CC1010 [31]	76.8Kbps Manchester Encoded	N/A
MICA Mote	TR1000 [30]	OOK 30Kbps / ASK 115.2Kbps	20-100m
MICAz Mote	CC2420 [34]	250Kbps	75-100m
MICA2 Motes [35]			
MPR400CB	CC1000 [25]	38.4Kbps Manchester Encoded	152.4m
MPR410CB	CC1000 [25]	38.4Kbps Manchester Encoded	304.8m
MPR420CB	CC1000 [25]	38.4Kbps Manchester Encoded	304.8m

Table V. Mote Power Profiles

Motes	**Transmit**	**Receive**	**Idle**	**Sleep**
EYES Mote	26.6mA	9.1mA	N/A	1μA
MICA Mote	12mA	3.8mA	N/A	0.7μA
MICAz Mote	17.4mA	19.7mA	20μA	1μA
MICA2 Motes				
MPR400CB	27mA	10mA	N/A	>1μA
MPR410CB	25mA	8mA	N/A	>1μA
MPR420CB	25mA	8mA	N/A	>1μA

2.2.2. Broadcast Radius The broadcast radius of a modeled transceiver can be changed by varying its transmission power and reception sensitivity. Varying the broadcast radius of the physical layer can have a large effect on the apparent performance of the MAC layer. Increasing the broadcast radius while maintaining the same spatial node density serves to increase the number of one hop neighbours an average node has. It has been shown [36] that increasing the number of one hop neighbours in a system that uses a shared medium increases the latency. Consider a contention based system; the probability of accessing the channel decreases with the number of nodes in the one hop area. The more nodes attempting to access the same channel, the greater the latency to obtain the channel and the greater the likelihood of collisions, resulting in greater latency. Decreasing the broadcast radius can also create problems from a routing perspective. With fewer one hop neighbours, nodes are constrained in the way in which they can route packets.

2.2.3. Power Model Another area that can have a large effect on the results presented is the power profile of the physical layer. Generally the power profile is quoted (if at all) as the transmit, receive, sleep and idle powers in Watts. Tuning the simulated power profile can dramatically change the results. Changing the ratio between the sleep, receive transmit and idle powers can artificially affect the observed energy efficiency. For example, by increasing the power cost of the idle state and reducing the cost of transmission, a MAC protocol that sends many control packets to coordinate the network may appear to be more efficient. It is interesting to note the discrepancies between the power profiles used shown in table III and the actual parameters as quoted in the radio transceiver data sheets shown in table V.

2.3. Routing

Routing is still an open issue in WSNs. It has been suggested that traditional naming schemes for nodes will be ineffective when a multitude of WSNs are in the network [37]. However central to all routing proposals is the concept that a node must decide to which neighbour (or subset of neighbours) it will forward a packet. The many different approaches taken in the surveyed protocols are displayed in table VI. There is a general split between optimal approaches as used in DMAC [6], S-MAC [29] and WiseMAC [22], and the more randomized approaches used in T-MAC [19] and TRAMA [20]. These approaches typify two of the three approaches that can be taken when dealing with the routing layer. Using an optimal approach seeks to negate the effect that the routing layer has on the presented performance of a MAC protocol. Using a randomized approach seeks to do the same whilst adding some of the randomness a real routing protocol may generate. The third approach is to use an existing routing protocol.

Table VI. Routing Protocols

MAC Protocol	**Routing Protocol**
DMAC [6]	Optimal Geographic
MERLIN [10]	EYES Source Routing (ESR)[38]
S-MAC [29]	Fixed Links
Sift [13]	Point to Point
Stem [15]	Optimal Geographic
T-MAC [19]	Randomized shortest path, no routing control packets.
TRAMA [20]	Random neighbour as next hop
WiseMAC [22]	Djikstra's Algorithm

2.4. Scenarios

An experimental scenario for evaluation of a WSN is described by the placement of nodes in the network (topology) and the different connections between nodes in the network (traffic parameters).

The topology of the network is an important factor to consider in simulation. The most basic topology pattern to investigate is local communication, both unicast and broadcast. The use of single-hop scenarios allows a developer to determine the performance of a protocol in isolation. This allows the investigation of its performance without concern for the multi-hop nature of sensor networks. One of the key mechanisms for data reduction in sensor networks, aggregation, relies on local broadcast and unicast of data. This makes investigation of the single-hop performance of MAC protocols for WSNs all the more pertinent. However, nearly all the reviewed papers fail to investigate the single-hop performance of their protocols.

Among the multi-hop scenarios that are investigated, the most popular is a random topology. The results achieved by investigating a network of randomly placed nodes in a particular area tend to be rather meaningless unless some important parameters of the model are provided. In general the performance of a MAC protocol degrades with the number of nodes in the network, but more specifically the performance at an individual node degrades with the number of local neighbours [36]. It should be essential for the evaluation of a random topology to disclose the average number of neighbours each node has in the simulation.

The placement of the sink in a WSN also has quite an effect on the results. In the surveyed papers, two suggested placements of sinks in random topology scenarios are the centre of the network or a corner of the network. Both of these placements produce different effects. If the nodes are randomly placed in the network one would expect that the node in the centre of the network would on average have 4 times as many neighbours as a node in the corner. Traffic flowing to a central sink is therefore prone to more contention, which would be expected to degrade the performance of the network. The typical traffic parameters used show an increase in traffic from some random source selected in the network to the sink.

Other non-random multi-hop scenarios are investigated in some papers. The two most popular are the multi-hop chain and multi-hop lattice topologies. The multi-hop lattice topology is essentially several over lapping multi-hop chain topologies. The key benefits of these scenarios are that they do not require any routing and due to their regularity they can be used to support simple mathematical estimates of the MAC layer behaviour.

2.5. Performance Metrics

MAC protocol performance can be gauged on the following metrics: power consumption, packet latency, scalability, throughput, fairness and support for mobility. The appropriateness of such metrics depends on the scenario being analysed. Ultimately, the performance metrics used to evaluate a MAC protocol allow the protocol developers to show the suitability of the protocol they have developed to the scenarios they have chosen to simulate.

Power Consumption In WSNs, where the lifetime of the network is based on the lifetime of the sensors, reducing power consumption is important. As a consequence power consumption is a key performance metric investigated in the evaluation of MAC protocols.

Latency *Single-hop latency* is defined as the average time spent by a packet in a MAC queue, from the time it is enqueued for scheduling until its transmission is complete. *End-to-end latency* is defined as the average time a packet takes to traverse a certain number of hops. Each is a function of both the protocol and the traffic characteristics and both are heavily affected by the sleeping time of nodes. In order to compare MAC protocols the traffic parameters must be kept consistent. Latency as a metric gives the network designer an idea of the immediacy of the applications they can expect the MAC layer to support.

Scalability A good MAC protocol for WSNs should be able to manage an extremely variable and possibly large number of devices. Due to the dynamic nature of such networks, scalability is an important metric to analyse. In fact, the number of sensors in a network may be in a constant state of flux due to node depletion and failure. Scalability can be evaluated by looking at the behaviour of the network when the one-hop node density is varied.

Packet overhead Packet overhead can be divided into data packet overhead and control packet overhead. Data packet overhead is caused by the generation of multiple copies of the same data due to broadcast and packet forwarding activity. Control packet overhead is due to control packets such as RTS, CTS, ACK, SYNC that the protocol employs for network management. Both data and control packet overhead enhance the communication reliability but also increase in latency and energy consumption. Packet overhead, which has been evaluated in the reviewed papers, can provide an insight into the specific protocol efficiency especially when evaluated in combination with energy consumption.

Support for Mobility Some WSN-specific applications require node mobility. At present, most MAC protocols for sensor networks assume a unique provider operating in each network area. This implies that issues like network handover can be ignored. Therefore, the problem of mobility support at the MAC layer can be combined with the problem of handling the unexpected presence/absence of neighbouring nodes. Furthermore, mobility support is tightly connected with the sleeping time of nodes. As a result, this metric can be evaluated by simply looking at the protocol scalability together with the single-hop packet latency.

Throughput Throughput is the fraction of the channel capacity used for data transmission. If the average message size is P bits, the average transfer time is T secs, and is the capacity of the channel is $C\ b/s$, then the throughput h is given by $h = P/TC$. Throughput can be measured on a single-hop basis, or it can be measured over a number of hops in the network. Throughput is an extremely important metric as it gives the network designer an idea of the applications that the network can support.

Fairness A MAC protocol which exhibits per-node fairness is one which has no preference for any single node when multiple nodes are trying to access the channel. In this way bandwidth is shared evenly amongst all nodes. However when traffic of different classes is being carried, e.g. multimedia traffic, fairness is the ability to distribute bandwidth in proportion to the requirements of the requesting nodes. None of the reviewed protocols use fairness as a metric when evaluating their protocols. Fairness is important in WSNs to ensure that all sensed phenomena are expediently reported.

3. BENCHMARK DEVELOPMENT

Using the survey conducted in the previous chapter, we are now in the position to make some suggestions regarding the design of an appropriate benchmark for WSNs. It is generally recommended that the parameters used during simulation should be comprehensive so that they not only show the choices a developer made for evaluation but also allow replication of the experiments using these parameters.

In order to obtain a comprehensive evaluation of a protocol, it is important to fully investigate the relationship between different network and protocol parameters. It is the duty of a benchmark to make an in-depth exploration of these often complex interdependencies.

The development of the benchmark is set out as follows. First the parameters to be set for simulation are presented, then the benchmark scenarios, and then specific metrics appropriate to each scenario. The purpose of each benchmark scenario is then clarified with respect to its metrics.

3.1. Simulation Environments

As mentioned in the background section 2 there are two preeminent simulation environments used in WSNs today ns-2 [2] and OMNeT++ [3]. It is not essential for protocol developers to use either of these two environments, but their open source status and strong community mean that developers can choose to release their protocol code to a wide audience of developers who will be able to experiment with it. This allows developers to independently test other developers' code, and determine cross layer performance.

The use of simulation brings the traditional problems of steady state simulation. Initialisation bias can be ameliorated by making the simulation runs long enough. The influence of initialisation bias is also further reduced with the number of times the simulation experiment is replicated [39]. The "method of independent replications" [40] should be used in all simulation experiments to ensure a rigorous confidence interval on the collected statistics of 95%. It is impossible to quantify in advance the number of independent runs necessary to achieve a specific confidence interval, as protocols may inject their own randomness into the experiments. Essentially, experiments are run, with different random seeds, until the confidence interval of the collected statistics is reduced to the acceptable level. OMNeT++ [3] provides methods to check for this in its "cStatistics" module.

3.2. Physical Layer

The most important recommendation to make for physical layer parameters is that the use of accurate parameters, for the chosen physical layer model, is paramount [41]. Currently the most popular radio transceivers used in Motes are the Chipcon CC1000 and CC1010. However as the physical layer technology continues to progress and evolve at a fast rate it is probable that these will soon be superseded. Therefore so as not to bias our benchmark towards one specific chip or chip manufacturer, we suggest using accurate data for the targeted physical layer platform. The accurate technical data for various mote platforms was presented in table IV at the time of publication. The references for the technical data sheets are included amongst the references.

It may seem that a benchmark in which the physical layer parameters are not set may make comparisons between different protocols using different physical layers difficult. However this problem can be addressed in the way the results are collected. To be able to make an accurate assessment of the power profile of a protocol, that is independent of the physical layer over which it operates, the following scheme can be utilized. Instead of only monitoring the amount of power that is used during a simulation, which is highly dependent on the physical layer, a better approach is to monitor the percentage of time the transceiver is in each of the following states: SLEEP, TRANSMIT, RECEIVE and IDLE. The number of transitions between states should also be tracked, as a transition between states requires a certain amount of power or *switching energy* [42]. This data can then be used to show how a specific node in the network behaves, or the network behaves as a whole, allowing a developer to determine the power profile for any specific proprietary physical layer model. If one knows the amount of power a physical layer uses when transmitting, receiving, idling and sleeping, then it is possible to estimate the power drain of a MAC protocol for a given period of time under a certain traffic load. This procedure was used in [29] to track the performance of their test bed radios.

Table VII summarises the most important fixed power model parameters of the physical layer.

Table VII. Physical Parameters

Physical Layer Parameters
Radio switching energy (E_{sw})
Tx energy (E_{tx})
Rx energy (E_{rx})
Idle energy (E_{idl})
Sleeping energy (E_{sl})

3.3. Average Node Degree

An important factor to consider when evaluating the performance of a multi-hop topology is the size of the average node neighbourhood (average node degree). This factor is often not explicitly considered in the evaluation of MAC protocols; more often only the average node density is considered. In the evaluation of a random scenario generally a paper will mention that n nodes were placed in an area Xm by Ym, giving a node density of $\frac{N}{X\,Y}$ m^2. This density metric can in fact be misleading. While it is certainly true that increasing the node density will increase the average amount of interference experienced by the nodes, the degree to which this interference increases is also determined by the interference/broadcast radius of nodes in the network and boundary effects, at the edges of the network. Boundary effects are a feature of both simulation and real networks and are illustrated in firgure 1. In this example the nodes labeled b and c experience the boundary effect. As nodes are only found within the area A the ability of these nodes to cover the areas marked in grey is superfluous. This causes a problem when attempting to determine the average node degree. To deal with this problem we present the formulation of a function that can be used to determine the network parameters required to achieve, on average, a specific broadcast/interference neighbourhood, or simply **average node degree**.

Initially one might expect that local phenomena would generalise to global phenomena when nodes are placed in an area in a uniform and random manner, implying the following ratio 1. In this equation d average node degree, n is the total number of nodes in the network, A is the total network area and r is the broadcast/interference ratio of the nodes.

$$\frac{d}{\pi\, r^2} = \frac{n}{A} \tag{1}$$

Unfortunately this ratio is inaccurate as it fails to take into account the boundary effects inherent in any rectangular area A. The inaccuracy occurs because of the assumption that every node covers an area of $\pi\, r^2$ with its broadcast/interference radius. While some nodes may cover an area of $\pi\, r^2$, due to boundary effects, nodes within distance r of the boundary will not. This effect means that the area covered by an average node must be less $\pi\, r^2$.

To determine the average area covered by a node one must first divide the area A up into 3 separate regions as shown in figure 2. If nodes are placed in a uniformly random manner the probability that a node will be placed in a sub area of A is the size of the sub area divided by the total area A. However let us first define A to be the area of a square of side lengths l such that equation 2 holds.

$$A = l^2 \quad \mathit{and} \quad l > 2\,r \tag{2}$$

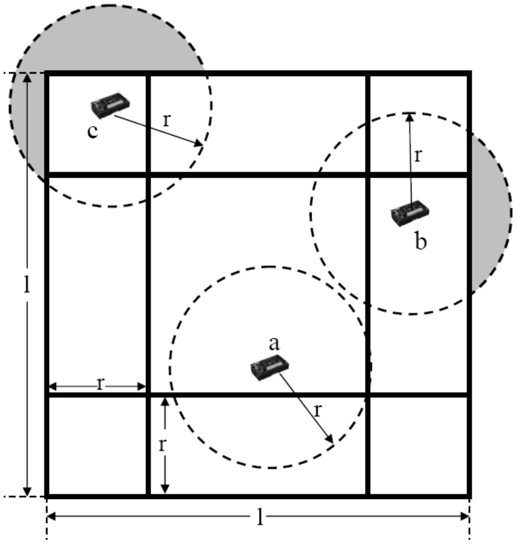

Figure 1. Boundary Effects in Network Area (A).

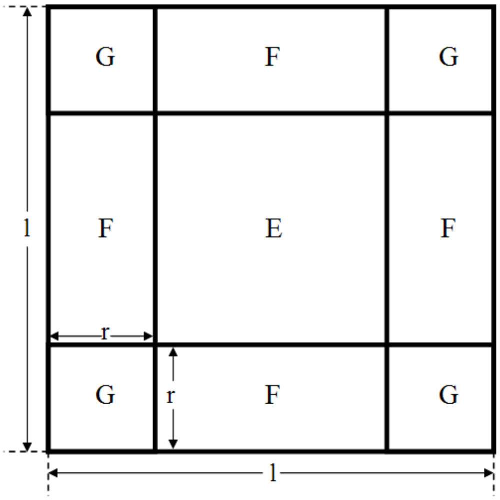

Figure 2. Network Area (A).

The first sub area to consider is the central sub area, E. E is chosen such that all points in E are at least a distance of r away from the border. The probability of a point being chosen in E is shown in equation 3 and nodes placed in this region cover an area shown in equation 4.

$$P(X, Y \,\epsilon\, E \subset \mathbb{R}^2) = \frac{(l-2\,r)^2}{A} \tag{3}$$

$$A(E) = \pi\, r^2 \tag{4}$$

Sub area F is comprised of the 4 marginal rectangles. The combined probability of a point being chosen in this area is shown in equation 5. Through integration of the integral in equation 6 the area that lies outside the network area can be summed. This sum can then be normalised over r to give the average area found outside the network area when a point is chosen in area F. It is possible to accurately determine the average area a node will cover within A by subtracting the result of this normalised integral from the total area of a circle, giving equation 7.

$$P(X, Y \,\epsilon\, F \subset \mathbb{R}^2) = 4\,\frac{(l-2\,r)\,r}{A} \tag{5}$$

$$\int_0^r r^2 \arccos(d/r) - d\sqrt{r^2-d^2}\,dd \tag{6}$$

$$A(F) = (\pi - 2/3)\,r^2 \tag{7}$$

Sub area G comprises of the 4 corner squares. Points will be chosen in this area with a probability shown in equation 8 and the average area covered by nodes chosen in this area can be estimated through simulation to be equation 9.

$$P(X, Y \,\epsilon\, G \subset \mathbb{R}^2) = 4\,\frac{r^2}{A} \tag{8}$$

$$A(G) = \frac{1}{3}\,\pi\,\sqrt{3}r^2 \tag{9}$$

Using these probabilities and average areas it is now possible to determine the average area of a point chosen in the entire network area A, described in equation 11. From this it is possible to create the ratio in equation 12.

$$C = P(E)\,A(E) + P(F)\,A(F) + P(G)\,A(G) \tag{10}$$

$$C = \frac{(l-2\,r)^2\ E}{A} + 4\,\frac{(l-2\,r)\ r\,F}{A} + 4\,\frac{r^2\,G}{A} \tag{11}$$

$$\frac{n}{A} = \frac{d}{C} \tag{12}$$

We can now use these results to design random topology simulation scenarios in which we can precisely vary the average density of the network nodes. Ideally the goal is to change the average interference/broadcast neighbourhood (average node degree) without changing the total number of nodes in the topology. In order to achieve this effect there are two options: varying the interference/broadcast radius r, or varying the network area A by changing the side length l. Either would have the desired effect. It is inadvisable to change the physical layer parameters as they should be kept consistent through all simulation scenarios. To determine how to change the area A the *quartic* function in l was formulated to equation 13. For a specific radius r, a total number of nodes n and a required density d, this equation can be used to find the side length l of the square network area A into which the network nodes will be uniformly randomly placed. The required side length l is the largest root of equation 13, as equation 2 must also hold. This root can be solved using the Ferrari method described in [43].

$$0 = 3\,dl^4 - 3\,nr^2\pi\,l^2 + 8\,nr^3 l + 12\,nr^4\pi - 16\,nr^4 - 4\,nr^4\pi\,\sqrt{3} \tag{13}$$

3.4. Scenarios

As discussed in the background chapter there are two categories of scenarios that have been investigated in the evaluation of WSN MAC protocols, single-hop and multi-hop. These are the two elementary scenarios in which a MAC protocol must function in a WSN. Here these scenarios are further formulated as part of a benchmark. The individual purpose of each scenario is also presented.

3.4.1. Single-hop Local communication is the building block of any multi-hop wireless network. Simulation of the single-hop scenario provides a baseline for more complex situations. As a measure of a MAC protocol, it shows how the protocol performs in isolation from the effects of routing. Local communication is particularly pertinent in WSNs as local broadcast and unicast are used for data aggregation. Several overlay protocols for WSNs have been suggested that use local clusters with a cluster head to mediate routing [44] or the MAC layer [45]. The communications between the cluster members and a cluster head are typically conducted in a local unicast manner, while the communications from a cluster head to cluster members typically utilise local broadcast. As such both local methods of communications are important and should be included in a benchmark. The suggested scenarios for benchmarking are outlined below. The parameters and metrics apply for both the unicast and broadcast scenarios.

Scenarios

1. **Local Unicast for Measurement of Channel Utilization:** Nodes are placed equidistant from a central node at a distance of $\frac{r}{2}$ so that all nodes interfere with each other (i.e. they are placed within the same transmitting range r). The central node is the sink to which all packets are sent.

2. **Local Broadcast for Measurements of Channel Utilization:** Nodes are placed equidistant from a central point at a distance of $\frac{r}{2}$ so that all nodes interfere with each other (i.e. they are placed within the same transmitting range r). No sink is used as all nodes broadcast.

Common Parameters

Duration: 1000 packets sent, each 100 bytes.

Variable: Number of neighbouring nodes. From 1 to 32.

Traffic: Nodes transmit as quickly as possible.

Experiments

Metric 1: Total Throughput (bps) vs. Number of Nodes.

Metric 2: Average per Node Throughput, Highest Throughput Node, Lowest Throughput Node, Standard deviation (bps) vs. Number of Nodes.

Purpose of Metric 1 for Scenario 1: To show how the MAC protocol behaves when saturated with unicast traffic. In the case where there are only 2 nodes (one source and one sink) it is possible to gauge the maximum performance of the MAC protocol in the absence of routing and interference from other nodes. This data point shows the best case point-to-point throughput that can be expected in the network. As the number of nodes increases it is possible to see how the MAC protocol being evaluated is able to handle the increasing interference on the channel. An ideal protocol would be able to sustain the throughput obtained in the 2 node case as the number of interfering nodes increases. However it is expected that for contention protocols the throughput will decay with an increase in the number of nodes.

Purpose of Metric 1 for Scenario 2: To show how the MAC protocol behaves when saturated with broadcast traffic. In the case when there is only one node transmitting it is possible to gauge the maximum performance of the MAC protocol in the absence of interference. As the number of the number of nodes increases it is possible to see how the MAC protocol handles increasing interference when broadcasting. An ideal protocol would be able to sustain the throughput of the one node case. However it is possible the throughput will decrease due to interference and collisions.

Purpose of Metric 2 for Both Scenarios: This experiment is intended to measure the fairness of the MAC protocol. The average per node throughput should be approximately $\frac{1}{n}$ of the total throughput as seen in the above experiment, where n is the number of nodes. This shows an estimation of the fairness of single-hop channel allocation. In fact, a good MAC should allow nodes to access the channel with equal probability so that it results in a low standard deviation of node throughput. Moreover, a good MAC protocol should produce a minimal number of collisions. By contrast, a bad MAC protocol tends to favour some nodes and starve others.

3.4.2. Multi-hop Multi-hop scenarios allow the simulation of the complex interactions that more closely approximate the nature of real world WSNs. The topology of the network is a key factor of the evaluation process. Often in the definition of a scenario the parameters of the topology reported are the total number of nodes in the network, the area of the network and the position of the sink. Unfortunately these parameters are not enough to allow cross-paper comparisons. A parameter often omitted, but key to understanding the performance of a network, is the node degree. The node degree is the number of neighbours a node is expected to have. As such it is a function of the node placement, the number of nodes in the network, the area the network is contained in and the nominal broadcast radius of the network. Experiments conducted with different random topologies but the same average node degree should show similar performance. The three scenarios that are proposed are two constrained scenarios (*chain* and *lattice*) and a less restricted scenario (*random topology*).

3.4.3. Chain In an ad hoc network, packets essentially travel along multi-hop chains between the source and the destination. These chains are determined by the routing protocol. Measuring the performance of one of these chains in isolation shows the upper level of performance that can be expected for a particular path in an ad hoc network. The only interference experienced in this network scenario is from the nodes of the chain themselves. It is possible for the utilization of the chain to be as high as $\frac{1}{3}$ of the two node point to point unicast throughput as seen in the single-hop scenario, if it is assumed that nodes that are not neighbours do not interfere with each other [36]. An ideal protocol would allow every third node to transmit simultaneously. Using a multi-hop chain scenario it is also possible to assess the latency incurred in an isolated scenario. It is possible to determine a function to assess the performance of an ideal MAC protocol under a multi-hop chain scenario. The formulation of such a function is presented below.

We define t_{tx} as the transmission time and t_{rx} as the reception time, with the assumption that $t_{tx} = t_{rx}$.

The time a packet takes to travel from the source to the sink is:

$$t_{e2e} = (n-1)t_{tx} \tag{14}$$

Where n is the total number of nodes in the network including source and sink, t_{e2e} is also the ideal end to end latency. Let d be the distance between neighbouring nodes, let r_b be the broadcast radius and let r_i be the interference radius. A node is only able to communicate with neighbours who are within a distance of r_b. If a node is receiving and is within the interference radius of another transmitting node, its attempt at reception will fail due to this interference. Here we assume that $r_b > d$ and $r_i < 2d$. If this is the case the minimum time the sink must wait before it can send its next packet is $3\,t_tx$ (since every third node may transmit simultaneously without interfering) as a result the minimum time between packets is t_{minp}.

$$t_{minp} = 3\,t_{tx} \tag{15}$$

Let t_{ia} be the inter-arrival time, where only $t_{ia} \geq t_{minp}$ is considered. It is now possible to determine how long the simulation will run. This value is called t_{sim}.

$$t_{sim} = \begin{cases} t_{e2e} + (p-1)t_{ia} & t_{ia} < t_{e2e} \\ p\,(t_{e2e} + (t_{ia} - t_{e2e})) & t_{ia} >= t_{e2e} \end{cases} \tag{16}$$

The behaviour of different types of nodes in the chain can now be determined. T_{sl}, T_{tx}, T_{rx} are the total amounts of time spent sleeping, transmitting and receiving for a particular network node, Sw is the number of times the radio switches state, and p is the total number of packets sent.

Source Behaviour

$$\begin{aligned}
&T_{sl} = t_{sim} - T_{tx}\\
&T_{tx} = p\, t_{tx}\\
&T_{rx} = 0\\
&Sw = 2\, p
\end{aligned}\tag{17}$$

Sink Behaviour

$$\begin{aligned}
&T_{sl} = t_{sim} - T_{rx}\\
&T_{tx} = 0\\
&T_{rx} = p\, t_{rx}\\
&Sw = 2\, p
\end{aligned}\tag{18}$$

Non-Terminal Node Behaviour

$$\begin{aligned}
&T_{sl} = t_{sim} - (T_{tx} + T_{rx})\\
&T_{tx} = p\, t_{tx}\\
&T_{rx} = p\, t_{rx}\\
&Sw = 4\, p
\end{aligned}\tag{19}$$

Total Network Behaviour

$$\begin{aligned}
&T_{sl} = n\, t_{sim} - 2\, p\, t_{tx}\, (1-n)\\
&T_{tx} = (n-1)\, p\, t_{tx}\\
&T_{rx} = (n-1)\, p\, t_{tx}\\
&Sw = (n-1)\, 4\, p
\end{aligned}\tag{20}$$

Average Node Behaviour

$$\begin{aligned}
&Av_{sl} = t_{sim} - \tfrac{(1-n)}{n}\, 2\, p\, t_{tx}\\
&Av_{tx} = \tfrac{(n-1)}{n}\, p\, t_{tx}\\
&Av_{rx} = \tfrac{(n-1)}{n}\, p\, t_{tx}\\
&Av_{sw} = \tfrac{(n-1)}{n}\, 4\, p
\end{aligned}\tag{21}$$

Average Node Power Consumption

$$P_n = Av_{sl}\, E_{sl} + Av_{tx}\, E_{tx} + Av_{rx}\, E_{rx} + Av_{sw}\, E_{sw} \tag{22}$$

For the multi-hop chain topology the suggested experiments are:

Scenario

Multi-hop Chain: 11 nodes [36] in a chain placed in such a way that the nodes are just within the broadcast radius of their neighbouring nodes. The node at the start of the chain generates the traffic, and the node at the end of the chain receives it.

Common Parameters

Duration: 1000 packets sent, each 100 bytes.

Variable: Traffic.

Sink: Node at the chain's end.

Experiment 1

Traffic: Inter-arrival time, varied from 0s to 10s.

Metric 1: Average per node Energy Consumption (J) and Standard Deviation % Sleep, Receive, Transmit, Idle vs. Inter-arrival Time (s).

Metric 2: Average End-to-End Latency (s) vs. Inter-arrival Time (s).

Purpose of Metric 1: Shows how much power is saved by sacrificing both latency and throughput. The data points at the beginning and end correspond to the latency end points of the latency metrics below. The standard deviation shows how fairly energy usage is distributed amongst nodes. The above ideal protocol parameters can be used as a performance comparison to the protocol under investigation.

Purpose of Metric 2: As latency is defined as the period of time between when the packet is initially queued and when the packet is finally delivered, this metric is used to determine how the MAC protocol affects latency under different queuing rates.

Experiment 2

Traffic: Lowest load (a new packet gets triggered when the packet reaches the destination) and heaviest load (all packets initially queued at the source).

Metric 1: Latency (s) vs. Number of Hops (shows the observed latency at each hop).

Metric 2: Throughput (bps) vs. Number of Hops (shows the observed throughput at each hop).

Purpose of Metric 1: This shows how the packets progress along the network. In a fair contention protocol packets should spend roughly the same amount of time at each hop and hence the graph should increase in a linear manner. This experiment is carried out on the lowest traffic load and the highest traffic load. The ideal latency should also be graphed for comparison.

Purpose of Metric 2: This metric is used to show any potential bottlenecks in the network. It is also possible to show how the MAC protocol handles bottlenecks using this graph. Ideally each link should have approximately the same throughput.

3.4.4. Multi-hop Lattice Lattice topology experiments provide a controlled yet more complex scenario than the simple multi-hop chain experiment presented above. The use of lattice topologies in investigating the performance of ad hoc wireless networks has been extensively studied [36] and used [22] for MAC protocol performance analysis. By maintaining a regular network topology and traffic pattern it is possible to estimate a nearly optimal global scheduling scheme, in the form of an ideal protocol, to compare with the actual performance of the MAC protocol that is being studied. Essentially the purpose of the lattice experiment is to see if the MAC protocol, in the absence of upper layer protocols, is able to allow different, interfering traffic flows to share the medium, and provide fair channel allocation to each flow. In a lattice topology, nodes are equidistant in the vertical and horizontal plane. That is to say, the distance between a node and its horizontal and vertical neighbours is s. Varying the distance s between nodes gives discrete neighbourhood sizes. We define two different types of neighbourhood. The broadcast neighbourhood of a node is defined as the set of nodes that are within its broadcast radius r_b. The interference neighbourhood is defined as the set of nodes that are within a distance of r_i of a particular node. Reciprocal communications are assumed, thus if a node n_i is in the broadcast neighbourhood of a node n_j, then n_j must be in the broadcast neighbourhood of n_i. The same argument can be used for the interference neighbourhood. The relationship between r (either r_i or r_b) and s can give the different discrete broadcast or interference neighbourhood sizes for non-terminal nodes in a regular lattice as shown in table VIII.

Table VIII. Relationship Between Radius, Internodal Distance and Neighbourhood Size in a Multihop Lattice

Relationship Between Radius (r) and the Internodal Distance (s)	**Neighbourhood Size**
$r < s < r\sqrt{2}$	4
$r\sqrt{2} < s < 2r$	8
$2r < s < r\sqrt{5}$	12
$r\sqrt{5} < s < 2r\sqrt{2}$	20
$2r\sqrt{2} < s < 3r$	24
$3r < s < r\sqrt{10}$	28
$r\sqrt{10} < s < r\sqrt{13}$	36
$r\sqrt{13} < s < 3r\sqrt{2}$	44
$3r\sqrt{2} < s < 4r$	48

In a multi-hop lattice there are multiple horizontal (or vertical) multi-hop chains. For communications purposes it is only necessary that non-terminal nodes are able to exchange data with their left and right neighbours. Therefore to determine the performance of a MAC protocol under such a scenario, the interference neighbourhood of the non-terminal nodes should be varied by changing the internodal distance s. This neighbourhood can be varied to the discrete levels shown in table VIII. It is recommended that a full analysis of the MAC protocol should vary the interference radius from the lowest possible level with 4 interfering neighbours through to 48 interfering neighbours. Each scenario should be evaluated under the same traffic load in order to give a basis for comparison. The average performance of equivalent non-terminal nodes (i.e. nodes with the same interference neighbourhood) should be analysed.

Scenario

Multi-hop Lattice: A 14 by 14 (to allow for the 48 neighbourhood size) regular lattice with nodes separated by distance s. Traffic is queued at the nodes on the far left side of the lattice, and travels to the right in parallel chains across the lattice to sinks on the right hand side.

Parameters

Duration: 100 packets sent from each source, each 100 bytes.

Variable: The size of the interference neighbourhood (node degree) which is varied from 4 – 48 by changing the internodal distance s to the incremental discrete levels shown in table VIII.

Sink: 14 sinks on the right hand side of the lattice.

Traffic: Poisson traffic generated with λ set at 1s.

Metrics

Metric 1: Average End to End Latency of Equivalent Multi-hop Chains (s) and Standard Deviation vs. Interference Neighbourhood.

Metric 2: Average Power Consumption of Equivalent Non-Terminal Nodes (J), % Sleep, Receive, Transmit, Idle vs. Interference Neighbourhood.

Metric 3: Average Throughput of Equivalent Multi-hop Chains (bps), Standard Deviation vs. Interference Neighbourhood.

Purpose of Metric 1: To show how multi-hop paths behave with respect to the latency as the amount of interference on these chains is increased.

Purpose of Metric 2: This experiment is used to show how the amount of power consumed by a non-terminal node is affected by the increase in the number of nodes that potentially interfere with it. Essentially all nodes should experience the same amount of interference and consequently the standard deviation should be low.

Purpose of Metric 3: To show how the traffic is shared amongst interfering multi-hop chains. In a fair protocol, the standard deviation should remain low.

3.4.5. Multi-hop Random Topology A multi-hop random topology can be used to show how a network is expected to perform in a more realistic scenario. To evaluate the protocol in a hypothetical application environment, a set of random topologies should be studied. The details of the simulation parameters, the node density, position of the gateway, transmitting range and the traffic models explored should be clearly stated. Below, some insights are given into how a random topology simulation should be conducted.

Traffic Models

Idle It may seem like a contradiction to include an idle traffic pattern. However it is possible that in certain WSN deployments, especially event reporting deployments, there may be sustained periods during which there is an "information drought" in the network. This may occur in both networks used to detect phenomena (when the phenomena are spaced far apart) or in networks used for periodical reporting (when the period is sufficiently high). Ideally a MAC protocol should keep energy expenditure at the physical layer to an absolute minimum during periods of information drought. As a result determining the performance of a MAC protocol idle is paramount to determining its suitability.

Periodic Reporting Traffic Periodic reporting is another mechanism which is expected to be supported by WSNs. This particular mechanism is pertinent especially to environmental monitoring applications which will periodically report the state of the environment to the sink. This traffic pattern can easily be modeled. Each node is given a periodicity using a Poisson process centred at the average reporting rate. The nodes then report back at the reporting rate they have been assigned.

Event Generated Traffic Phenomenon detection is a central mechanism which is expected to be supported by WSNs. When a phenomenon is detected, the sensing nodes report it to the sink node. It is possible that nodes' sensing areas overlap with each other and one or more nodes may detect and report the same phenomenon. While it is possible that this data may be aggregated at a higher level, a well designed MAC protocol for WSNs should be able to handle geographically co-located instantaneous bursts of traffic. To simulate this effect, a phenomenon is defined as a point p with a radius r. When a phenomenon is triggered any node within the area described by the circle with centre p and radius r will report the phenomenon to the sink. These phenomena will arrive with a Poisson inter-arrival time and be uniformly and randomly distributed throughout the network area. Equation 23 can be used to determine the radius r of such a phenomenon in order to simulate a scenario where on average e nodes are triggered by each phenomenon. Equation 23 is solved where n is the number nodes in the network, l the network area side length and e is the average number of nodes to be triggered by each phenomenon. Equation 23 is a rearrangement of equation 13 where e replaces d. A phenomenon is essentially an invisible node that triggers nodes within its radius, and works in the same way as the broadcast/interference radius mechanism.

$$0 = (12\,n\,\pi - 16\,n - 4\,n\,\pi\sqrt{3})\,r^4 + 8\,n\,l\,r^3 - 3\,n\,\pi\,l^2\,r^2 + 3\,e\,l^4 \tag{23}$$

Routing

The three broad routing options discussed for multi-hop WSN scenarios were optimal routing, randomized routing and the use of an actual routing protocol. Any of these options is a viable choice as long as they are used in a consistent manner. In general a MAC protocol analysed using a randomized routing protocol will be difficult to compare to a protocol analysed an optimal routing protocol. The recommendation of this benchmark is to either use a specific actual routing protocol, especially if you are developing for your protocol to interact with one or to use an optimal protocol. Optimal protocols are preferable to randomized protocols as real protocols aim to be optimal, but never aim to be random.

Network Lifetime Estimation

In order to estimate the total network lifetime, we must first determine what constitutes the end of a network lifetime. Each sensor node has a certain power supply. In most cases this is a pair of AA (R6) batteries which can be expected to each have a voltage of 1.5V and a rating of 2000mAh. This means that the total power supply has a ration of 3V (v_{node}) for 2000mAh (p_{batt}). The lifetime of the network will end when some fraction of the nodes in the network have exhausted their power supply. Ideally one would like to select this fraction such that when this fraction of nodes has expired the network becomes disconnected. However this is rather difficult as this fraction will be unique for every unique random topology simulated, and in some cases as low as one node in the network. With this in mind the criteria we shall use is that the network lifetime t_{life} is bounded by that of the most active node: for the sake of measurement, the network lifetime is considered expired when the first node exhausts its power supply. This represents the lower bound on the potential network lifetime. We can estimate the network lifetime from the equation 24. In this equation e_i is the energy a node consumes in state i in mW, t_i is the energy a node consumes in state i, t_{sim} is the duration of the simulation, and a_{node} is the current drain of the node in mA.

$$\begin{aligned} p_{node}(mW) &= \frac{\sum_{i \in States} e_i\, t_i}{t_{sim}} \\ a_{node}(mA) &= \frac{p_{node}}{v_{node}} \\ t_{life}(h) &= \frac{p_{batt}(mAh)}{a_{node}} \end{aligned} \tag{24}$$

Each of the suggested scenarios to be tested in this random topology section will have 100 sensor nodes and 1 sink node. The 100 sensor nodes will be uniformly and randomly distributed throughout the network area A. The parameters for the network area are shown in table IX.

Table IX. Simulation Parameters

Density	**Sparse**	**Medium**	**Dense**
Nodal Degree (d)	4	12	24
Total Number of Nodes (n)	100	100	100
Broadcast Radius (rm) [25]	304.8	304.8	304.8
Network Side Length (lm)	2561	1409	939
Network Area (Am^2)	6558721	1985281	881721
Phenomenon Radius for e=2 (rm)	212	117	77

Scenario

Multi-hop Random Topology Network: 100 nodes scattered in an area so as to make a sparse, medium and dense network.

Common Parameters

Duration: 1000s (so on average each node will have sent 100 packets, each 100 bytes).

Sink: One sink located in the bottom right hand corner of the network.

Variable: The average node degree, by varying the network area.

Experiment 1

Traffic: Idle.

Metric: Average Power Consumption (J), Standard Deviation of Power Consumption, % Sleep, Idle, Receive and Transmit vs. Average Node Degree.

Purpose of Metric: This experiment allows the comparison of the performance of various MAC protocols under the condition of an information drought in the network. Ideally a protocol should use as little power as possible. When power is used, it is also desirable to know how it is used. This can be determined by the percentage of time the protocol is in Sleep, Receive, Transmit or Idle states and the distribution of power expenditure can be seen in the Standard Deviation.

Experiment 2

Traffic: Periodic reporting traffic with Poisson periodicity of 10s. (so on average each node will send 100 packets.)

Experiment 3

Traffic: Event-generated traffic, phenomena occur with a Poisson inter-arrival time of 0.2s and an e of 2. (so on average each node will send 100 packets.)

Metrics

Metric 1: Average Per Hop Latency (s), Standard Deviation vs. Average Node Degree

Metric 2: Estimated Network Lifetime (hours) vs. Average Node Degree

Purpose of Metric 1: The average per hop latency allows the network designer to determine if this MAC protocol will be on average able to meet the required performance criteria. The standard deviation shows how variable the performance is likely to be. By evaluating this metric with the following lifetime we can determine how the performance is traded off against the energy savings.

Purpose of Metric 2: The network lifetime gives the final estimation of how long the network can operate with full connectivity.

4. DISCUSSION

The benchmark scenarios presented in section 3 can be used to conduct a thorough evaluation of a MAC protocol. The single-hop scenarios in section 3.4.1 probe the limits of the local throughput performance. They are used to show the upper limit of point-to-point performance, and how the throughput performance decays as the MAC protocol handles an increasing amount of interference from neighbouring nodes. The multi-hop chain scenario in section 3.4.3 investigates the trade off between energy efficiency and both latency and throughput. It is also used to determine how the protocol performs as the amount of traffic through a multi-hop link is increased. The multi-hop lattice scenario in section 3.4.4 extends upon the multi-hop chain scenario by determining the performance of multi-hop chains as they forward traffic in parallel. These controlled scenarios provide a valuable insight into the performance of the MAC protocol when it is isolated from the effects of upper layer protocols. The multi-hop random topology scenarios in section 3.4.5 provide an investigation of how a MAC protocol can be expected to behave when deployed in a real WSN. Combined, these scenarios expose the relationship between the energy-efficiency and performance of MAC protocols for WSNs.

5. CONCLUSION

There are many and varied potential applications for WSNs, each of which have their own requirements. Thus the comprehensive assessment of MAC protocols for WSNs complicated. The lack of any common benchmarking standard makes the cross-comparison of MAC protocols difficult. The goal of this paper has been to introduce a benchmark to simplify the comparison of MAC protocols and hopefully pave the way for development of new protocols. To achieve our goal, the current methods of evaluating the performance of MAC protocols for WSNs were surveyed. From the survey the key scenarios and performance metrics were distilled. These performance metrics were explored in relation to the scenarios to which they are appropriate. The benchmark describes how both single-hop and multi-hop scenarios can be investigated, to thoroughly evaluate a MAC protocol. A novel approach to calculating the average node degree is presented for multi-hop random scenarios. The method is shown to also be useful for the generation of event based traffic. This allows for a more consistent investigation of multi-hop random scenarios for WSNs. The proposed procedure of benchmarking aims to greatly improve the quality of MAC protocol assessment and rectify the present lack of common agreement between researchers and developers of the area. Ultimately the success of a benchmark is measured by the number of its adherents.

ACKNOWLEDGEMENTS

Many thanks to the Smart Internet Technology CRC for their continuing support. Special thanks to Dan Cutting and Adam Hudson for their efforts proof-reading this paper.

REFERENCES

1. G. J. Pottie and W. J. Kaiser. Wireless integrated sensor networks. *Communications of the ACM*, 43:51–58, 2000.
2. Steven McCanne and Sally Floyd. ns Network Simulator. http://www.isi.edu/nsnam/ns/.
3. A. Varga. The OMNet++ discrete event simulation system. In *European Simulation Multiconference*, Prague, Czech Republic, June 2002. http://www.omnetpp.org.
4. Joseph Polastre, Jason Hill, and David Culler. Versatile low power media access for wireless sensor networks. In *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 95–107. ACM Press, 2004.
5. Berkley Mote. http://www.cs.berkeley.edu/ awoo/smartdust/.
6. Bhaskar Krishnamachari Gang Lu and Cauligi Raghavendra. An adaptive energy-efficient and low-latency MAC for data gathering in sensor networks. In *Wireless, Mobile, Ad Hoc and Sensor Networks (WMAN 04)*, April 2004. DMAC.
7. Van Hoesel, Chatterjea, and Havinga. An energy efficient medium access protocol for wireless sensor networks. *proRISC 2003*, November 2003.
8. IEEE P802.15.4/D18. Draft standard: Low data rate wireless personal area networks. Technical report, IEEE, February 2003.
9. P. J. M. Havinga, L. F. W. van Hoesel, and S. Chatterjea. A low-latency, information-centric medium access protocol for wireless sensor networks. In *ProRisc*, The Netherlands, November 2004. L-MAC.
10. A.G. Ruzzelli, G.M.P OHare, M.J. OGrady, and R. Tynan. Merlin: A synergetic integration of mac and routing protocol for distributed sensor networks. *To appear in Third Annual IEEE Communication Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks SECON06*, Sept 2006.
11. Andre Barroso, Utz Roedig, and Cormac J. Sreenan. mu-MAC: An energy-efficient medium access control for wireless sensor networks. In IEEE Computer Society Press, editor, *Proceedings of the 2nd IEEE European Workshop on Wireless Sensor Networks (EWSN2005), Istanbul, Turkey*, February 2005.

12. T. Zheng, S. Radhakrishnan, and V. Sarangan. Pmac: an adaptive energy-efficient mac protocol for wireless sensor networks. In *Proceeding of 19th IEEE International Symposium Parallel and Distributed Processing*, pages 95–107. IEEE, 2005.
13. Kyle Jamieson, Hari Balakrishnan, and Y. C. Tay. Sift: A MAC protocol for event-driven wireless sensor networks. Technical report, MIT, May 2003. Sift.
14. Wei Ye, John Heidemann, and Deborah Estrin. An energy-efficient MAC protocol for wireless sensor networks. In *Proceedings of the IEEE Infocom*, pages 1567–1576, New York, NY, USA, June 2002. USC/Information Sciences Institute, IEEE. S-MAC.
15. Curt Schurgers, Vlasios Tsiatsis, Saurabh Ganeriwal, and Mani Srivastava. Optimizing sensor networks in the energy-latency-density design space. *IEEE Transactions on Mobile Computing*, 1(1):70–80, 2002. Stem.
16. R. Bagrodia and R. Meyer. PARSEC: A parallel simulation environment for complex system. *Computer Magazine*, 1998.
17. C. Suh and Y.-B. Ko. A traffic aware, energy efficient MAC protocol for wireless sensor networks. In *IEEE ISCAS*, May 2005.
18. Crossbow Technology. MICA mote. Technical report, Crossbow Technology, San Jose, CA, USA, 2005.
19. T. V. Dam and K. Langendoen. An adaptive energy-efficient MAC protocol for wireless sensor networks. In *SenSys*, pages 171–180, Los Angeles, CA, 2003. T-MAC.
20. Venkatesh Rajendran, Katia Obraczka, and J. J. Garcia-Luna-Aceves. Energy-efficient collision-free medium access control for wireless sensor networks. In *SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems*, pages 181–192, New York, NY, USA, 2003. ACM Press. TRAMA.
21. Scalable Networks. Qualnet. http://www.scalable-solutions.com.
22. A. El-Hoiydi and J.-D. Decotignie. WiseMAC: An Ultra Low Power MAC Protocol for the Downlink of Infrastructure Wireless Sensor Networks. In *Proceedings of the International Symposium on Computers and Communications ISCC*, pages 244–251, Alexandria, Egypt, June 2004. WiseMAC.
23. R. Bagrodia, X. Zeng, and M. Gerla. GloMoSim: a Library for Parallel Simulation of Large-scale Wireless Networks. In *Proceedings of the International Workshop on Parallel and Distributed Simulationm*, pages 154–161, May 1998. GloMoSim.
24. Mahesh Aia Injong Rhee, Ajit Warrier and Jeongki Min. Zmac: a hybrid mac for wireless sensor networks. In *SenSys '05: Proceedings of the 3nd international conference on Embedded networked sensor systems*. ACM Press, 2005.
25. Chipcon. CC1000 datasheet. Technical report, Chipcon AS, Oslo, Norway, May 2005.
26. Gang Lu, Bhaskar Krishnamachari, and Cauligi Raghavendra. Performance evaluation of the IEEE 802.15.4 MAC for low-rate low-power wireless networks. In *Workshop on Energy-Efficient Wireless Communications and Networks (EWCN '04)*, April 2004.
27. Koen Langendoen and Gertjan Halkes. *Embedded Systems Handbook*, chapter Energy-Efficient Medium Access Control. CRC press, August 2005.
28. NORDIC. nRF2401 datasheet. Technical report, Nordic, 2002.
29. Wei Ye, John Heidemann, and Deborah Estrin. Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Trans. Netw.*, 12(3):493–506, 2004.
30. RF Monolithics. TR1000 datasheet. Technical report, RF Monolithics, Dallas, TX, USA, July 2003.
31. Chipcon. CC1010 datasheet. Technical report, Chipcon AS, Oslo, Norway, May 2005.
32. A. Ribordy T. Melly, E. Le Roux, F. Pengg, D. Ruffieux, N. Raemy, F. Giourd, and v. Peiris. WiseNET: Design of a low-power RF CMOS reciever chip for wireless applications. Technical report, CSEM, 2002.
33. A. G. Ruzzelli, L. Evers, S. Dulman, L. F. W. Van Hoesel, and P. J. M. Havinga. On the design of an energy-efficient low-latency integrated protocol for distributed mobile sensor networks. *IWWAN International Workshop on Wireless Ad hoc Networks*, June 2004.
34. Chipcon. CC2420 datasheet. Technical report, Chipcon AS, Oslo, Norway, May 2005.
35. Crossbow Technology. MICA2 datasheet. Technical report, Crossbow Technology, San Jose, CA, USA, May 2005.
36. J. Li et al. Capacity of ad hoc wireless networks. In *ACM/IEEE MOBICOM*, pages 61–69, 2001.
37. Chalermek Intanagonwiwat, Ramesh Govindan, and Deborah Estrin. Directed diffusion: a scalable and robust communication paradigm for sensor networks. In *Mobile Computing and Networking*, pages 56–67, 2000.
38. J. Wu, P. Havinga, S. Dulman, and T. Nieberg. Eyes source routing protocol for wireless sensor networks. *Proceeding of European Workshop on Wireless Sensor Networks EWSN*, January 2004.
39. David Goldsman. Simulation output analysis. In *WSC '92: Proceedings of the 24th conference on Winter simulation*, pages 97–103, New York, NY, USA, 1992. ACM Press.
40. A. Francini and F. Neri. A comparison of methodologies for the stationary analysis of data gathered in the simulation of telecommunication networks. In *Modeling, Analysis, and Simulation of Computer and*

Telecommunication Systems, 1996. MASCOTS '96., Proceedings of the Fourth International Workshop on, pages 116–122, 1996. TY - CONF.

41. G. Anastasi, A. Falchi, A. Passarella, M. Conti, and E. Gregori. Performance measurements of motes sensor networks. In *MSWiM '04: Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems*, pages 174–181, New York, NY, USA, 2004. ACM Press.
42. Antonio G. Ruzzelli, Pablo Cotan, Richard Tynan, and Gregory O'Hare. Protocol assessment issues in low duty cycle sensor networks: and switching energy. *Under revision of the 1st International conference on sensor networks and trustworthy computing (SUTC06)*, 1, January 2006.
43. D. E. A. Smith. *Source Book in Mathematics*. Dover, New York, 1994.
44. Ya Xu, John Heidemann, and Deborah Estrin. Geography-informed energy conservation for ad hoc routing. In *MobiCom '01: Proceedings of the 7th annual international conference on Mobile computing and networking*, pages 70–84, New York, NY, USA, 2001. ACM Press.
45. D. J. Corbet and D. Everitt. A partitioned power and location aware MAC protocol for mobile ad hoc networks. In *European Wireless*, Nicosia, Cyprus, April 2005.

AUTHORS' BIOGRAPHIES

Derek J. Corbett

Derek Corbett received a Bachelor of Advanced Science with first class honours in Computer Science from the University of Sydney in 2003. Currently he is a Ph.D. candidate at the University of Sydney, under the supervision of Prof. David Everitt. His research is sponsored by the Smart Internet Technology CRC. In 2005 he was granted a DAAD stipendium for a six month exchange to RWTH University Aachen, Germany. He is currently working on the use of location awareness in ad hoc networks, with a focus on the interplay of location and both MAC protocols and service discovery protocols.

For further information see: http://www.derekjay.net

Antonio G. Ruzzelli

Antonio Ruzzelli received a 5 years laurea degree (equivalent to a masters) in Electronic Engineering with a specialisation in telecommunications at the University of Ferrara, Italy, 2005. In 2004, he received a one year for grant to work on the European EYES project for energy-efficient sensor networks at the University of Twente (Netherlands). At present he is a Ph.D. candidate at University College Dublin, Ireland, supervised by Prof. Gregory O'Hare. He is working on the Adaptive Information Cluster (AIC) project. His work is focused on resilient and reliable protocols for energy-efficient and adaptive WSNs. Ancillary projects include fixed broadband wireless access (FWBA) based on the IEEE802.16a standard known as WiMax technology through collaboration with the Performance Engineering Laboratory (PEL) at UCD/DCU, Dublin, Ireland.

For further information see: http://www.cs.ucd.ie/students/aruzzelli/default.htm

Prof. David Everitt

David Everitt holds the position of Chair of Internetworking at the University of Sydney.

He received the degrees of B.E. and Ph.D. in Electrical Engineering from the University of Queensland in 1976 and 1981 respectively. He worked from 1981 to 1986 at British Telecom Research Laboratories, from 1987 to 1988 at Telecom Australia Research Laboratories, from 1989 to 2000 at the Department of Electrical and Electronic Engineering, The University of Melbourne, Australia, and from 2000 to 2001 as Professor, Convergent Technologies at Swinburne University of Technology, Melbourne, Australia. He has been at University of Sydney since 2002. He has been editor for Wireless Network Performance for IEEE Transactions on Communications 1996–1999, and has served on the technical program committees of many international conferences.

His research interests are in performance engineering for communication networks, especially with regard to wireless communications networks, local area networks, and all-optical networks.

For further information see: http://www.it.usyd.edu.au/d̃everitt

Prof. Gregory O'Hare

Gregory O'Hare is a Senior Lecturer in the School of Computer Science & Informatics at University College Dublin. He was previously a member of faculty at the University of Manchester Institute of Science and Technology (UMIST), UK. He is director of the PRISM (Practice and Research in Intelligent Systems & Media) Laboratory within the School of Computer Science & Informatics. His research focuses upon Multi-Agent Systems (MAS) and Mobile & Ubiquitous computing. He has published over 200 journal and conference papers in these areas together with two text books and has secured over 11 Million Euros in research funding. O'Hare is an SFI Investigator, managing with others a cluster of research awards to the value of some 9 Million Euros in the area of Adaptive Information.

For further information see: http://csiweb.ucd.ie/Staff/AcademicStaff/gohare

School of Information Technologies, J12
The University of Sydney
NSW 2006 AUSTRALIA
T +61 2 9351 4917
F +61 2 9351 3838
www.it.usyd.edu.au

ISBN 1 86487 863 0