PERIODIC DATA DISSEMINATION IN WIRELESS SENSOR NETWORKS: A THEORETICAL APPROACH

GRAHAM WILLIAMSON[1], DAVIDE CELLAI[2], SIMON DOBSON[3], PADDY NIXON[2]

[1] *Systems Research Group, School of Computer Science and Informatics, University College Dublin, IE*
[2] *Lero, School of Computer Science and Informatics, University College Dublin, IE*
[3] *School of Computer Science, University of St. Andrews, Scotland, UK*
{*Email: graham.williamson@ucd.ie*}

Abstract: Epidemic-based communications, or "gossiping", provides a robust and scalable method for maintaining a knowledge base in a sensor network faced with an unpredictable network environment. Since sensed information is often periodic in time, protocols should be able to manage multiple messages in an efficient way. In this paper we review some recent findings of network epidemic processes and propose a mathematical model of gossiping dealing with multiple messages. We present simulation results that suggest the model can provide insights into the design and optimisation of sensor networks in the case of dissemination of periodically generated data. We address issues of network topology, data lifetime, data freshness and communications overhead. In particular, we show that it is possible to control data freshness without increasing overhead, and quantify the importance of topology in achieving timely dissemination.

Keywords: Gossiping; Network science; Autonomic systems; Mathematical modelling; Epidemics

1 INTRODUCTION

Wireless sensor networks (WSNs) [1, 2, 3] pose particular problems of robustness and tolerance of component failures. The network must remain functional despite losses of individual links and nodes, and must retain and transport sensed information. Since most WSNs involve battery- or self-powered nodes, efficient power utilisation is also critical in order to maintain sensor and network longevity. Long lifetimes must however be balanced against the desire to measure the events that the network has been deployed to sense. This complicates power management decisions.

Epidemic communications – "gossiping" [4, 5, 6, 7, 8] – can provide an effective means of transferring data around a WSN. Gossiping replaces the traditional producer/consumer model of networks, in which consumers request information from sensors, with a flatter peer-to-peer structure in which information is propagated and replicated between nodes. This has many advantages, including better management of the load and an improvement of robustness and performance [4]. However, the scheme also impacts the power consumption, storage, bandwidth, data integrity and freshness of the network. Consumers cannot explicitly request the most up-to-date information, and conversely may expend resources maintaining information in which they have no interest. A principal component of data integrity is providing bounds on the time taken for sensed data to percolate through the network and reach consumer nodes. Moreover, since many of these trade-offs vary dynamically, WSNs require significant autonomic management [9].

The problem of information dissemination on networks goes well beyond the area of WSN. There has been a growing interest in recent years in large networks as a paradigm for describing most diverse systems such as large scale infrastructures (power grids, telecommunication networks, etc...), social acquaintances, biological interactions of genes or proteins, molecular or particle gels. General properties of networks have been formalized into mathematical models and have been studied by methods of natural sciences. This broad area of knowledge is often referred to as *network science* [10, 11]. Epidemic dissemination of viruses or other types of information has also been explored using this approach and several results have deepened our understanding of such problems [12, 13]. Our aim is applying insights given by network science to gossiping on WSN.

In this paper we present a new simple model of gossiping on a WSN. The model describes dissemination and interaction of periodically sensed data, which are distributed by gossiping without increasing the traffic on the network. The model also allows to control data freshness and to define the best sampling frequency. Moreover, the model is a useful tool to explore the effects of network topology and size. We employ techniques widely used in physical and life sciences – and indeed part of our intention is to expose these techniques more widely within the computer simulation community.

Section 2 briefly describes gossiping in the context

of WSN management, and section 3 presents our new model, the Multi-Rumour Overwriting (MRO) model. Section 4 presents simulation results for different network topologies, while section 5 concludes with some future directions for this work.

2 BACKGROUND

2.1 Gossiping

In many systems the communications patterns observed in a network follow the function that the system implements, in the sense that (for example) communications will be targeted by consumer nodes and information-producer nodes, with the producers of more "interesting" information receiving more traffic. This approach is simple, intuitive and modular, but poses two significant problems:

1. **Hot spots and hot paths.** Nodes can become overloaded with requests for service, both as end-points and through routing traffic. WSNs are typically not able to deploy the techniques of virtualisation and replication used in enterprise systems, and so will tend to see their performance degrade.

2. **Single points of failure.** If a node serves the data it collects, its failure will result in data loss. Many replication strategies are subject to pathological failure cases, exacerbated by relatively poor connectivity between nodes.

The intuition behind gossiping is to remove this link between traffic and function. In a gossiping-based system, nodes periodically synchronise with another node – typically a neighbour, but also possibly a more remote node – chosen at random. The two nodes exchange data, possibly with some consistency checking or consolidation. Information sensed by one node will therefore propagate across the network through a series of gossiping exchanges. Under certain conditions (detailed below), all nodes will eventually receive all information, allowing them to answer queries by accessing purely local information. Gossiping has a number of attractive features. The random nature of communications removes hot spots and hot paths, whilst the pervasive replication of data makes the system relatively immune to local failures or changes in node populations and connectivity ("churn"). The challenge, therefore, is to address issues of data freshness and lifecycle in order to leverage these advantages.

The topic of formulating flexible and reliable gossiping protocols has attracted considerable interest in recent times. Among the many approaches, the work by Levis *et al.* [14] presents a very efficient algorithm, named *Trickle*, which is reminiscent of gossiping models widely applied in social networks [15]. With *Trickle*, the two typical problems of disseminating information to all nodes in a sensor network (to change sensor sampling times, install new code, or send management commands, for example) and collection of information towards a single sink node in the sensor network (for processing or forwarding outside the network) are both cast in such a way that they can be solved by implementing a protocol of eventual consistency. Gossip-based communication provides an elegant solution to this problem. *Trickle* implements an adaptive protocol which increases or decreases the speed of contact between nodes based on information appearing in the network.

Many other gossip and non-gossip style protocols exist for the dissemination of information across sensor networks. The SPIN family of protocols [16] addresses the problems of message implosion and energy conservation. Directed Diffusion [17] tackles dissemination in a non-gossip style, setting up communication gradients over which information is routed towards interested nodes. Barrett *et al.* [18] gave us probabilistic protocols which take into account network information in setting the probabilities for information retransmission. However, the goal in their case is routing of information towards a single collection sink, rather than dissemination across all nodes. More recently, RAPID [19] uses probabilistic forwarding and gossip-based eventual consistency in conjunction with parametrically controlled retransmission probabilities (based on local density as in [20]) to provide a practical dissemination protocol for wireless networks.

A possible problem of gossiping is that the information available locally may not be the most recent available in the network, and this poses challenges for some applications whilst being perfectly acceptable for others. It may also require aggressive data management and/or relatively larger per-node memory to cope with the replication inherent in the gossiping exchanges, since otherwise each node would potentially be required to hold *all* the information available *anywhere* in the network. In this paper, we focus on the particular problem of disseminating periodically sensed information to all nodes across a WSN. Our aim is to study the effect of network topology and to present a simple model able to control the age of the diffusing messages, without increasing network traffic.

2.2 Information propagation in networks

The analysis of a general gossiping system involves relating the propagation of information to the topological properties of the network. This is a problem encountered in many domains and, as we mentioned in the introduction, may be tackled using methods inspired by network science.

The number of edges going out of a node is called its *degree*. The most important characterisation of the

network topology is the degree distribution $P(k)$, the probability that a randomly-chosen node has degree k. The tail of the degree distribution at high k plays an important role in characterizing the properties of the network. A simple example is a random graph, also known as the Erdős-Rényi model, which can be represented as a network with Poisson degree distribution

$$P(k) = \exp(-z)\frac{z^k}{k!}$$

where z is the mean degree [11]. This distribution represents the standard topology of a network without correlations. Another important degree distribution is the power law $P(k) \sim k^{-\alpha}$. Because of the absence of a characteristic scale (a typical degree which measures the speed of the decay), the corresponding networks are called scale-free. Scale-free networks constitute one of the most common topologies in many real networks or, in other words, many real networks can be approximated by a scale free topology [10, 11]. It is interesting to remark that the Internet at the router level has been considered scale free with exponent about 2.5 [21]. Recently, however, this topology has been strongly argued [22]. The difference between these two distributions is shown in Figure 1.

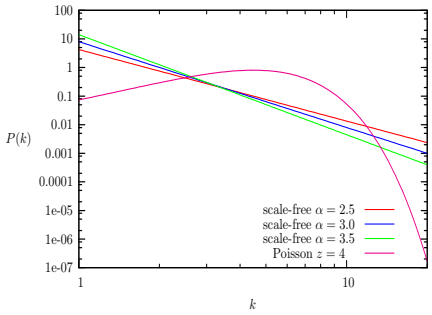


Figure 1: Comparison between scale free and Poisson distributions. The Poissonian vanishes much faster than any power law (log-log scale).

Erdős-Rényi networks can be generated by randomly attaching node pairs with probability p. Their distribution represents the standard topology of a network without particular correlation. It can be considered the normal distribution for networks. Scale-free networks are also very common in many disciplines. An important characteristic of scale-free networks is the fat tail of the distribution, which even implies an infinite standard deviation for $\alpha \leq 3$. This means that the number of highly connected nodes, or hubs, tends to be very high in finite networks and tends to infinity for larger and larger networks. Such characteristic plays a very important role in information dissemination, as we discuss below.

In epidemiology, such network topologies are used to study the spread of disease infections through a population, with nodes representing people and edges representing social contact. This is clearly similar to the propagation of information through gossiping in a communications network, so similar methods can be used to analyse the critical parameters and how they affect the information flow [8]. Two of the simplest models describing such processes are the SIR and the SIS model [11].

The SIR model is the simplest model of an *epidemic* disease such as influenza in society or a virus in a computer network. At any time each node is in one of three possible states: *susceptible* (S), meaning they are healthy, but they can catch the disease if exposed to it; *infective* (I), meaning they have the disease and can pass it on and *recovered* (R), meaning they have caught the disease but have become immune, so that they can neither catch it nor pass it on. The disease spreads from an infective (I) node to the adjacent susceptible nodes with probability β and each infective node has a probability to become immune (R) equal to some constant γ. Without loss of generality, one can set $\gamma = 1$ and define $\lambda = \beta/\gamma$ as infection rate. The general question about the SIR model is whether the network will end up with a large major fraction of recovered nodes, or most of them will remain susceptible. These behaviours can be described by saying that there is an *epidemic threshold*. This means that there is a critical value of the infection rate λ which discriminates between two regimes: if the infection rate is higher than λ, the infection spreads throughout the entire network, and otherwise dies out. One of the most important findings about the SIR model is the absence of an epidemic threshold for large scale-free networks with an exponent of the power law which is less than 3. This means that the epidemic will always occur, no matter how small the infection rate is [12]. The SIS model is the simplest model for *endemic* disease, in which nodes transition from susceptible, to infective, and then become susceptible again instead of achieving immunity. Here the equivalence with the epidemic transition of the SIR model is a phase transition between the phase in which the disease vanishes and the one where it persists.

3 THE MRO MODEL

Information flow in a WSN is quite similar to these two models, but in the case of WSNs there are clearly some complications. On one hand, we wish to consider different pieces of information (e.g. different sensor observations) propagating through the network simultaneously. This is an important practical issue that traditional models do not address and we believe that a thorough theoretical investigation can be of great assistance in improving existing algorithms. On the other hand, differently from epidemic models, we *seek* complete infection of the network rather than seeking to *avoid* it. For the purposes of autonomic management, we wish to identify the impact of different parameters on the ways in which information

spreads. We refer to spreading information as a *rumour*, and consider single and multiple rumour systems.

We represent a WSN in a very simplified way: every sensor constitutes a node in a network and the edges between nodes connect sensors which are within their communication range. As a further simplification, we assume that sensor movement is not an important issue. This second requirement can also be regarded as the hypothesis that sensors move much slower than data and messages, and network topology does not change qualitatively. Now the goal is not to understand the spreading of a disease, nor to elaborate strategies of preventing an outbreak; on the contrary, the aim is to obtain a high fraction of recovered nodes at the end of the process, possibly with a minimum amount of traffic.

Rumour spreading has been studied by a number of theoretical approaches [23, 24, 15, 25]. A possible approach is to modify the SIR model as in Moreno *et al.* [15], where infective nodes remain infective until they attempt to communicate with *another* infective or recovered node: such a node then recovers with a rate γ. Otherwise an infective node continues to spread the rumour indefinitely.

In this context, *reliability* is defined as the final fraction of recovered nodes: a network is more reliable if it has a higher fraction of nodes that hold the information.

We propose a different approach, which aims to be more realistically close to the behaviour of WSNs. Our model is a modification of the SIS model, where the infection rate λ represents the probability that at each time step a node sends a rumour to one of its neighbours. This cannot be generally set to one, since we consider the possibility of fluctuations of the coverage range, due to temporary or permanent obstacles, intermittent battery power, etc. Differently from the SIS model, though, nodes do not get back to a susceptible state (becoming similar to the SI model). This can be considered a problem for practical implementations, because in real WSNs sensed information has not infinite validity, but there is a maximum time beyond which it becomes surely unreliable. However, we will see later that this issue is taken care of by an overwriting procedure.

The main novelty of the model is the fact that we do not consider a single rumour, but a set of them generated by the same node with period $\Delta\tau$. Moreover, as soon as a rumour touches a node infected by a different rumour, the newer overwrites the older. This characteristic describes a scenario quite common in sensor networks, where we want more recent data to overwrite older data that may still be propagating. An example may be periodic updating of firmware running on the sensor nodes, where every sensor needs just the latest update, and not all the old updates inserted in the network.

The advantages of the model are:

1. Information is fresher on average than with a single rumour.
2. There is no overhead due to checking the statuses of the neighbouring nodes to decide on further spreading of the rumour.

We refer to this model as the Multi-Rumour Overwriting (MRO) model. The MRO model was implemented in Java and experiments were conducted using the *Peersim* [26] discrete event simulator.

4 RESULTS

4.1 Dissemination characteristics

As an initial step, we have tested the behaviour of the MRO model on uncorrelated networks, taking into consideration Erdős-Rényi and scale-free topologies.

In the case of scale-free networks, we define the degree distribution as $P(k) = (\alpha - 1)m^{\alpha-1}/k^{\alpha}$, where $m = 2$ is the minimum degree and α is the power law exponent. The networks have been generated by implementing an algorithm to obtain uncorrelated networks without multiple edges and self-connections [27] – fairly obvious properties for WSNs. For this reason, the maximum degree M has always been set $M \lesssim N^{1/2}$, where N is the number of nodes.

At the beginning of each simulation, a random node is chosen as a starting point of the generated rumours. Rumours are created sequentially with a period $\Delta\tau$. In Figure 2, we compare the time evolution of the fraction $i_s(t)$ of infected nodes by a single rumour with the one produced by several rumours $i(t) = \sum_{r=1}^{n} i_r(t)$, generated every $\Delta\tau = 12$. We consider a network of scale-free topology with $\alpha = 3$ and infection rate $\lambda = 0.1$. This choice of the parameters is only an illustrative example. It can be seen that the model has a smooth behaviour with respect to λ, whereas the choice of $\Delta\tau$ is convenient because it is comparable to the characteristic time of the epidemic spreading. Accordingly, what we are interested here is to show the qualitative behaviour of the model. Once the general patterns are understood, this work can be useful in designing protocols where parameters are tailored to suit the specific problem.

In the case of single rumour, the fraction of nodes which receive the message for the first time increases monotonically as in an avalanche-like behaviour: first the infection propagates slowly, then it grows very rapidly, and finally slowly saturates. In the multi-rumour case, we also observe a three step growth of the global fraction of infected nodes. The time required to sweep the whole network is roughly the same as in the case of single rumour, and the discrepancy appears to be a random fluctuation. This similar behaviour coexists with the fact that the fraction

of sites containing a given type of rumour never gets close to 1. The reason is that every infective node spreads randomly any information with the same infection rate, and every rumour originates from the same node. On the other hand, rumour overlapping does not increase the traffic per unit time, because the overwriting rule eliminates every duplicate. Indeed, it is quite clear from Fig. 2 that it is not necessary to impose an explicit maximum age for rumours, because when rumour frequency is high enough, a spontaneous overwriting of old rumours occurs.

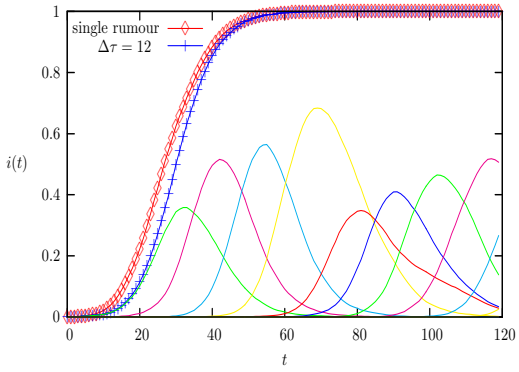


Figure 2: Time evolution of the fraction of infected nodes i in a scale free network with exponent $\alpha = 3$, total number of nodes $N = 10^3$, and infection rate $\lambda = 0.1$. Results are averaged on 10 different simulations, with a different randomly chosen injection node. The red diamonds represent the fraction of infected nodes in a single rumour scenario. The blue crosses represent the total fraction of infected nodes in the network, in simulations where the rumours are generated with period $\Delta\tau = 12$. The other curves represent the fraction of nodes infected by a particular rumour.

As a check, we investigate the behaviour of the model in the case of short message life. We set a maximum age τ_a for each rumour, after which the rumour automatically expires. In order to test the effect of this parameter, we consider the case in which τ_a is smaller than the typical lifetime of a rumour in the network. In Fig. 3 we show a simulation on an $\alpha = 3$ scale free network, with $\tau_a = 30$ and $\Delta\tau = 3$, and we compare it with a single rumour with the same maximum age. The characteristic time of the outbreak is not very different from the single case. In both simulations the infection does not reach every node. The reason is that since the next rumour always starts from the same point, there is a maximum path that they can travel in the interval τ_a, which corresponds to a maximum fraction of nodes they can reach. Increasing the rumour frequency, the initial growth of i becomes less and less steep, but the fluctuations around the stationary value get smaller. This demonstrates that introducing an explicit maximum age for the rumours does not add any benefit to the protocol, because the same effect can be achieved by tuning the frequency of rumour generation with a better performance in terms of network coverage.

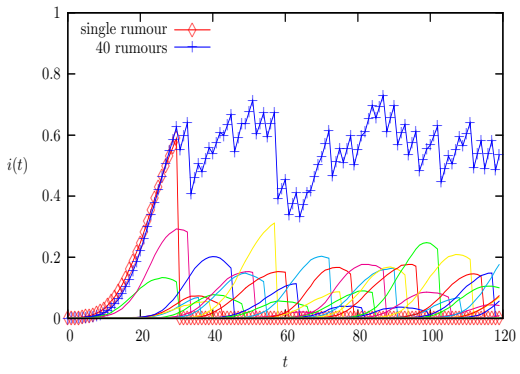


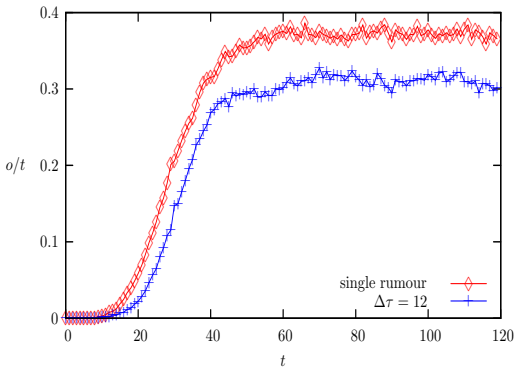
Figure 3: Infected node evolution for a $\alpha = 3$ scale free network with $N = 1000$, $\lambda = 0.1$, $\Delta\tau = 3$ and $\tau_a = 30$. The single rumour case is represented as a comparison by the red diamonds. Lower curves are the infective fractions of each rumour.

Returning to the case study of Figure 2, we define the overhead of the dissemination by counting the number of "useless contacts", *i.e.* the contacts between an infective node and another node infected by the same rumour or a newer one. In figure 4(a) we show the comparison of overheads. The one with multiple rumours has lower overhead per unit time than the case with single rumour. The overhead is significantly reduced by the fact that in a large number of contacts a newer rumour replaces an older one. In fact, the mean message age grows initially up to a constant value, which depends on the rumour frequency ($1/\Delta\tau$) and the infection rate λ (figure 4(b)).

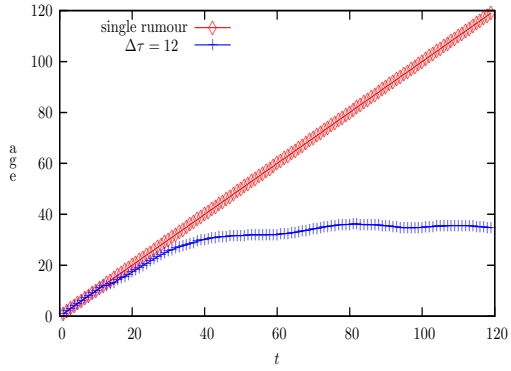
The inflection point on the curve $i(t)$ can be considered a measure of the characteristic time of the dissemination (Fig. 2). In order to improve effectiveness, it may be desirable to choose the node where to start the dissemination from. We consider the degree k as a criterion to choose this injection node. Fig. 5 shows how the characteristic time depends on the degree of the injection node. We observe that the characteristic time decreases with the degree, as expected. It is interesting to note, however, that the improvement of choosing a higher degree initial node is less and less important for increasing k, so that there is not a substantial difference, in the given example, between $k = 25$ and $k = 40$. This trade-off should be taken into account to improve the protocol efficiency.

4.2 Control of message freshness

We have seen that each node in the network, after a transient period, receives a new message which overwrites the older ones within a range of time intervals which oscillates around a mean value. We can express this concept by defining the mean age of mes-



(a)



(b)

Figure 4: Comparison between the single- and many-rumour scenario. Parameters are as in Fig. 2. (a) Overhead per unit time versus time. (b) Time evolution of the mean age of rumours stored on the nodes.

sages stored on the nodes in the network. This characteristic of the network can be fully controlled by tuning the parameters λ and $\Delta\tau$. In Fig. 6 we show the dependence of the mean rumour age on the message generation period $\Delta\tau$, for different values of infection rate λ. The simple linear behaviour allows to easily determine the rumour frequency necessary to obtain a desired mean message age. We can also observe two interesting properties. First, the slope of the curve does not appear to depend on the topology, and even the absolute values of the mean age are very similar. Second, the protocol is perfectly scalable with network size. In fact, comparing the plots for two different orders of magnitude in network size (Figures 6(a) and 6(b)), it is evident that this characteristic line remains very stable both in terms of slope and actual age values. This striking scalability is due to the fact that, generally speaking, rumour age on a given node does not depend on the distance (e.g. shortest path) from the injection point (and thus the network size), but only on the delay between two different "waves" of rumour copies. Moreover, the mean time spent by a rumour on a node essentially depends only on λ and the shortest path between two successive infected regions, which is fairly independent from the topology. Hence, the low influence of topology on the characteristic curve.

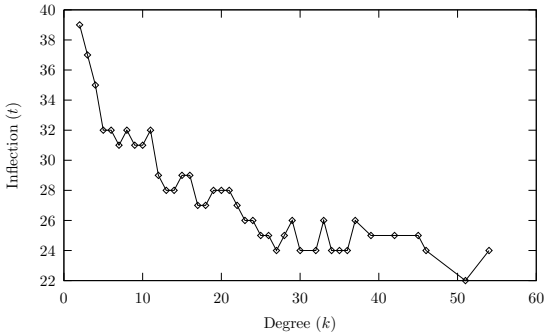


Figure 5: Characteristic time of a $\lambda = 0.1$ dissemination (calculated as the inflection point of $i(t)$) versus degree of the injection node. Scale-free network with $\alpha = 3$ and $N = 10^4$.

Our results also indicate that mean rumour age quickly converges to a fixed value by increasing the infection rate (see Fig. 7). In fact, there is a minimum life time of each rumour which depends on $\Delta\tau$ and the network topology. In the case of a fully connected clique (every node attached to every one else), this value reaches the lowest possible mean age of $\Delta\tau/2$. This implies that beyond a certain small value of λ, the value of the infection rate does not add anything any more to the mean freshness of circulating information. This can be important in WSN design: a too high λ only increases power dissipation without improving the sensed information.

4.3 Topology comparison

We have compared the behaviour of the model with different network topologies. In figure 8, $i(t)$ is plotted for a single rumour for scale-free networks with $\alpha = 2.5, 3, 3.5$ and an Erdős-Rényi network, characterized by a Poissonian distribution $P(k) = \exp(-z)z^k/k!$, where we choose the parameter z roughly close to the mean degree of the scale-free networks (to be able to check the sole effect of the standard deviation). Decreasing the value of α, information dissemination becomes easier, and the rapidity of the infection increases, as expected. Quite interestingly, the behaviour of the evolution of i in an Erdős-Rényi graph is in between the ones of the scale free networks. One would rather expect a slightly slower growth [13]. The reason is due to the small size of the considered networks ($N = 10^3$), which magnifies the importance of finite-size effects. Indeed, simulations of larger networks (as in Fig. 9 for $N = 10^4$) show that the avalanche shifts to lower times for $\alpha = 3$ and $\alpha = 2.5$.

A wireless sensor network rarely involves more than 1000 components, meaning that it is not always advisable to assume the validity of properties which have been demonstrated for infinite network sizes. Topology affects the characteristic time of the infec-

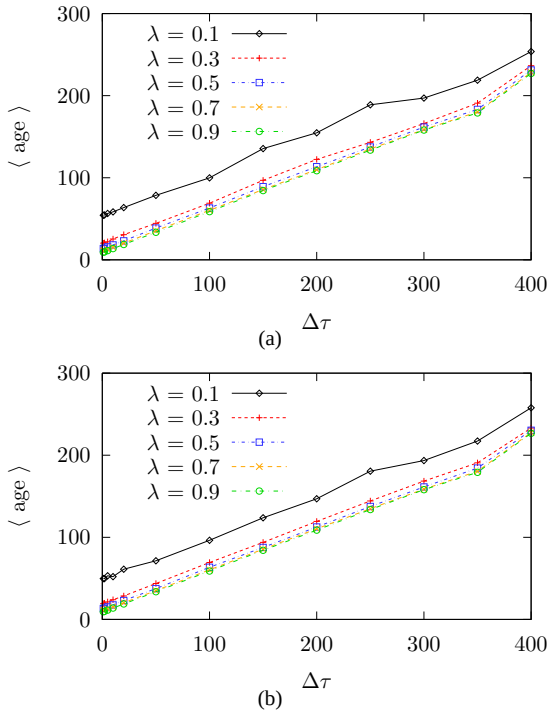


Figure 6: Mean rumour age versus $\Delta\tau$ for different infection rates λ. Scale-free network with $\alpha = 3$ and size $N = 10^3$ (a) and $N = 10^4$ (b), respectively.

tion in a complex way. Dissemination is very fast in large scale-free networks with $\alpha \leq 3$, but for $\alpha > 3$ Erdős-Rényi graphs may be more effective. Also, epidemic spreading is more effective in Erdős-Rényi networks with higher average degree, because there is a greater fraction of highly connected nodes, which enhances the dissemination.

It is also interesting to look at the overhead per unit time plotted in the inset of Fig. 8. Consistently with the behaviour of $i(t)$, the overhead is characterized by a three step behaviour. In the second stage of the evolution, the slope of the overhead per unit time of the scale-free networks decreases by increasing the exponent α. The reason is that the dissemination becomes less and less rapid because the "hubs" of

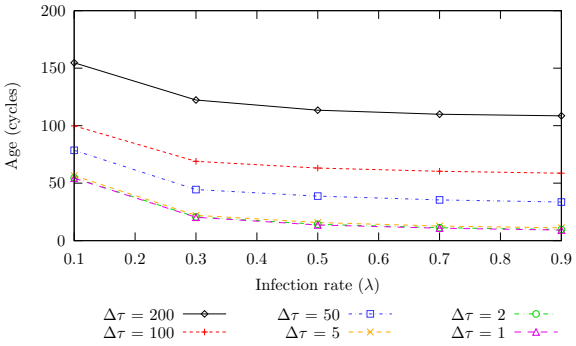


Figure 7: Mean rumour age versus infection rate λ for different values of $\Delta\tau$. Scale-free network with $\alpha = 3$ and size $N = 10^3$.

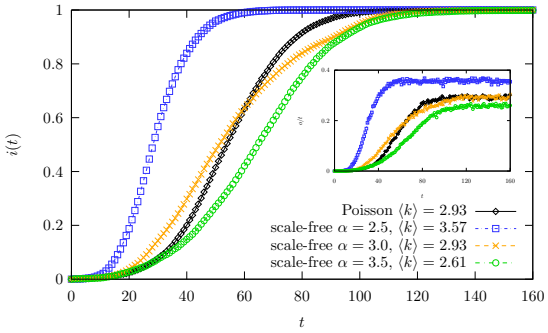


Figure 8: Time evolution of infective nodes for networks with different topologies ($\langle k \rangle$ is the measured mean degree). Single rumour scenario, $\lambda = 0.1$, and $N = 10^3$. The inset shows the overhead per unit time for the same topologies.

the network have lower connectivity on average. The Erdős-Rényi network takes on average more time to exhibit significant overhead, because of the smaller amount of highly connected nodes. Then, the overhead per unit time gets quickly to saturation, at a constant which equals $\lambda\langle k \rangle$, the mean number of infected nodes per unit time in the steady state.

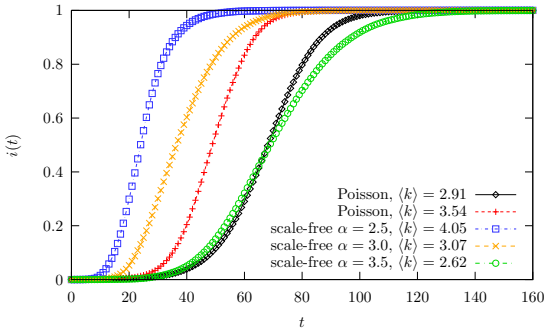


Figure 9: As in Fig. 8, but for $N = 10^4$.

It is tempting to conclude that, quite surprisingly, a relatively sizeable network of 1000 nodes still does not show an extremely strong dependence of dynamical properties from topology issues. Indeed, from our simulations it emerges that topology influences the characteristic time of gossiping with a factor around 2, which can be easily compensated by an improvement of the infection rate. This underlines the generality of this approach, that can be applied to a number of different problems in sensor and computer networks.

5 CONCLUSIONS

In this paper we have presented simulation studies of the way in which an information base with frequent updating of sensed data can be maintained using gossiping in a WSN. The proposed model is an attempt to find a novel strategy to optimise data dissemination in WSNs. This strategy consists in multiple overwriting

rumours which are randomly spread from a node to its adjacent neighbours. This scheme does not affect the reliability of the dissemination or the global traffic, but improves the average freshness of information stored in the nodes. Moreover, it allows us to control the novelty of distributed information, efficiently managing the traffic and limiting the diffusion of old messages. As a further advantage, the model allows us to simply control the amount of old information without forcing it explicitly.

Whilst most work on gossiping has occurred in the domain of overlay networks (for example [6]), such techniques may be inefficient in case of a very different physical network. In fact, it may be impossible to deploy a WSN according to a scale-free or a Poissonian topology, even though it may be desirable for rapid dissemination. However, it should be observed that a random deployment of identical sensors constitutes an Erdős-Rényi network by definition, provided the communication range is large enough to ensure the formation of a large connected cluster. Investigating the topology of typical deployments, and links between topology and behaviour form a key challenge for the future. A natural direction of further research is also to focus on node failure.

Finally, we have observed that the model deals with static networks: some degree of local movement does not affect the basic results, as long as the time scale is much larger than the time of sweeping the whole network and the topology is not completely changed. Moreover, localized movements may also be represented by a lower infection rate λ. In a more thorough study of this problem, the mobility of nodes must be taken into account, allowing some degree of rewiring of the network over time: if sensors can move, they may leave the coverage area of some sensors and get connected with others. Apart from such improvements, the MRO model appears to be a general, efficient approach to data dissemination in WSNs with periodic sensed information.

ACKNOWLEDGMENT

This work is supported by Science Foundation Ireland under grant 07/CE/I1147, and 03/CE2/I303-1, “Lero: the Irish Software Engineering Research Centre.”

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” *Computer Networks*, vol. 38, pp. 393–422, 2002.

[2] D. Culler, D. Estrin, and M. Srivastava, “Overview of sensor networks,” *Computer*, vol. 37, pp. 41–49, 2004.

[3] C. S. Raghavendra, K. M. Sivalingam, and T. F. Znati, *Wireless sensor networks*. Springer, 2006.

[4] A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart, and D. Terry, “Epidemic algorithms for replicated database maintenance,” in *PODC ’87: Proceedings of the sixth annual ACM Symposium on Principles of distributed computing*, 1987, pp. 1–12.

[5] P. T. Eugster, R. Guerraoui, A. Kermarrec, and L. Massoulie, “Epidemic information dissemination in distributed systems,” *Computer*, vol. 37, pp. 60–67, 2004.

[6] M. Jelasity and O. Babaoglu, “T-Man: fast gossip-based construction of large-scale overlay topologies,” Department of Computer Science, University of Bologna, Tech. Rep. UBLCS-2004-7, 2004.

[7] A. Kermarrec, A. Ganesh, and L. Massoulie, “Probabilistic reliable dissemination in large-scale systems,” *IEEE Trans. Parall. Distr. Syst.*, vol. 14, pp. 248–258, 2003.

[8] W. Vogels, R. van Renesse, and K. Birman, “The power of epidemics: robust communication for large-scale distributed systems,” *ACM SIGCOMM Comp. Comm. Rev.*, vol. 33, pp. 131–135, 2003.

[9] S. Dobson, S. Denazis, A. Fernández, D. Gaïti, E. Gelenbe, F. Massacci, P. Nixon, F. Saffre, N. Schmidt, and F. Zambonelli, “A survey of autonomic communications,” *ACM Transactions on Autonomous and Adaptive Systems*, vol. 1, no. 2, pp. 223–259, December 2006.

[10] R. Albert and A. Barabási, “Statistical mechanics of complex networks,” *Rev. Mod. Phys.*, vol. 74, p. 47, 2002.

[11] M. E. J. Newman, “The structure and function of complex networks,” *SIAM Review*, vol. 45, p. 167, 2003.

[12] R. Pastor-Satorras and A. Vespignani, “Epidemic spreading in scale-free networks,” *Phys. Rev. Lett.*, vol. 86, p. 3200, 2001.

[13] M. Barthélemy, A. Barrat, R. Pastor-Satorras, and A. Vespignani, “Velocity and hierarchical spread of epidemic outbreaks in scale-free networks,” *Phys. Rev. Lett.*, vol. 92, p. 178701, 2004.

[14] P. Levis, E. Brewer, D. Culler, D. Gay, S. Madden, N. Patel, J. Polastre, S. Shenker, R. Szewczyk, and A. Woo, “The emergence of a networking primitive in wireless sensor networks,” *Commun. ACM*, vol. 51, no. 7, pp. 99–106, 2008.

[15] Y. Moreno, M. Nekovee, and A. F. Pacheco, "Dynamics of rumor spreading in complex networks," *Phys. Rev. E*, vol. 69, p. 066130, 2004.

[16] W. R. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," in *MobiCom '99: 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, 1999, pp. 174–185.

[17] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in *MobiCom '00: 6th annual international conference on Mobile computing and networking*, 2000, pp. 56–67.

[18] C. L. Barrett, S. J. Eidenbenz, L. Kroc, M. Marathe, and J. P. Smith, "Parametric probabilistic sensor network routing," in *WSNA '03: 2nd ACM International Conference on Wireless Sensor Networks and Applications*, 2003, pp. 122–131.

[19] V. Drabkin, R. Friedman, G. Kliot, and M. Segal, "Rapid: Reliable probabilistic dissemination in wireless ad-hoc networks," in *SRDS '07, 26th IEEE International Symposium on Reliable Distributed Systems*, 2007, pp. 13–22.

[20] A. Khelil, C. Becker, J. Tian, and K. Rothermel, "An epidemic model for information diffusion in manets," in *MSWiM '02: 5th ACM international workshop on Modeling analysis and simulation of wireless and mobile systems*, 2002, pp. 54–60.

[21] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On power-law relationships of the internet topology," in *SIGCOMM '99: Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication*, vol. 29, no. 4. New York, NY, USA: ACM, October 1999, pp. 251–262. [Online]. Available: http://dx.doi.org/10.1145/316188.316229

[22] W. Willinger, D. Alderson, and J. C. Doyle, "Mathematics and the internet: A source of enormous confusion and great potential," *Notices of the AMS*, vol. 56, no. 5, May 2009. [Online]. Available: http://www.ams.org/notices/200905/rtx090500586p.pdf

[23] D. J. Daley and D. G. Kendal, "Stochastic rumours," *J. Inst. Math. Appl.*, vol. 1, pp. 42–55, 1965.

[24] D. H. Zanette, "Dynamics of rumor propagation on small-world networks," *Phys. Rev. E*, vol. 65, p. 041908, 2002.

[25] M. Nekovee, Y. Moreno, G. Bianconi, and M. Marsili, "Theory of rumour spreading in complex social networks," *Physica A*, vol. 374, pp. 457–470, 2007.

[26] M. Jelasity, A. Montresor, G. P. Jesi, and S. Voulgaris, "The Peersim simulator," http://peersim.sf.net.

[27] M. Catanzaro, M. Boguñá, and R. Pastor-Satorras, "Generation of uncorrelated random scale-free networks," *Phys. Rev. E*, vol. 71, p. 027103, 2005.