Introducing Epidemic Models for Data Survivability in Unattended Wireless Sensor Networks

Roberto Di Pietro*
Università di Roma Tre
Department of Mathematics
Roma, Italy
dipietro@mat.uniroma3.it

Nino Vincenzo Verde
Università di Roma Tre
Department of Mathematics
Roma, Italy
nverde@mat.uniroma3.it

***Abstract*—One of the most relevant issues pertaining UWSN is to guarantee a certain level of information survivability, even in presence of a powerful attacker. In this paper, we provide a preliminary assessment of epidemic-domain inspired approaches to model the information survivability in UWSN. In particular, we show that epidemic models can be used to set up the parameters that allow the information to survive, once estimated the maximal compromising power of the attacker. Further, we point out that the mere application of these models is not always the right choice. Indeed, it comes out that these deterministic models are not enough accurate, and "unlikely" events can cause the loss of the datum. Finally, we provide some final comments, as well as promising research directions.**

***Keywords*-Unattended Wireless Sensor Network, Epidemic Models; Data Survivability.**

I. Introduction

Unattended Wireless Sensor Networks (UWSNs) are Wireless Sensor Networks characterized by the sporadic presence of the sink. Sensors collect data from the field, and then they try to upload all the information they currently store as soon as the sink comes around [1]. Typical scenarios take into account monitoring systems to detect the presence (or the absence) of a subject, or the modification of a certain physical parameter [2]. An example is a monitoring system to detect poaching in a national park, as well as a monitoring system to check the pressure of an underground pipeline. In both these examples, a traditional Wireless Sensor Network (WSN) is not suitable. Indeed, the dimension of the area is prohibitive in the former case, while technical problems to connect the sink with underground sensors arise in the latter. Due to the absence of a direct and alive connection with the sink, these networks are more subject to malicious attacks than traditional WSNs. Without providing adequate security mechanisms, an adversary could compromise a set of sensors during the sink absence, deleting from the sensor memory some data, and leaving the sensor. These activities could be conducted without leaving evidence of their occurrence. Hence, one of the relevant problems in an UWSNs is to provide a certain level of assurance about the *information survivability*. Indeed, an adversary goal could be to prevent a sensed information from reaching the sink.

Unattended WSNs, and more in general WSNs, can generate periodic or event driven data. In the first case, sensors send to the sink periodic packets regarding the area they are monitoring, while in the second case they send a packet only if a particular event is detected. The choice of the model to use strongly depends on the purpose of the network. When dealing with monitoring issues, probably an event driven protocol is preferable. Indeed, on the one hand, if the events to detect are sporadic, sensors can save a great quantity of power. On the other hand, event driven protocols hardly detect malfunctioning of the sensors, issue that is easily addressable using periodic messages. In this paper, we will consider scenarios where the event driven choice is more effective.

To assure information survivability, *cryptographic* or *non-cryptographic* approaches can be used. Often the choice depends on the sensors that are going to be used in the network. Cryptographic approaches are suitable for high-end sensors, that are equipped with a pseudo number generator, and that can rely on a considerable computational power. Non-cryptographic approaches are suitable for low-cost sensors, that do not have the capability to execute computational intensive calculation. Generally, facing up with non-cryptographic protocols is more challenging, above all when trying to minimize the power consumption. Indeed, these protocols usually have to exchange more messages when compared with those based on cryptographic techniques. In this paper, we will focus exclusively on non-cryptographic approaches for information survivability.

Contribution

The main contribution of this paper is to assess the feasibility of epidemic models in order to enforce information survivability in an UWSN. In particular, we first show that modelling an UWSN via epidemic models is meaningful. Later, we define two attacker models and show that two specific epidemic models do well capture the introduced

[*] *He is also with CNR-IIT Security Group, Pisa, Italy.*

978-1-4577-0351-5/11/$26.00 ©2011 IEEE

attacker models. Further, we show that when trying to minimize energy consumption, optimal parameters choice in standard models do not assure the intended data survivability. This is generally due to “unlikely” events, that are not considered in the deterministic epidemic modelling, but that must be considered in our settings. Moreover, we strive to derive the parameters that achieve these two conflicting goals: to minimize the waste of bandwidth —and therefore the energy consumption—introduced by such models; and, to assure information survivability. Experiments do support our analytical findings. Finally, we highlight some further research directions.

Organization of the paper

Section II surveys related work in the area, while Section III introduces the two epidemic models that will be leveraged to model information survivability in UWSN—the SIR model is discussed in Section III-A, while the SIS model is discussed in Section III-B. In Section IV, we detail the features of the UWSN that we are going to consider, and we show that the transmission in this network corresponds to the disease-spreading in epidemic models. Section V leverages on the SIR and SIS model to set up the parameters that assure information survivability, while Section VI highlights the problems that have to be taken into account when using these deterministic models. Finally, Section VII reports some concluding remarks.

II. Related work

Epidemic models have already been leveraged in broadcasting and gossiping protocols for WSNs [3], but our target is quite different: rather than having each sensor storing the datum, we are interested in that *at least* one sensor stores it.

Kermack and Mckendrick [4] used for the first time a mathematical formulation to predict the spreading of diseases within a population. The mathematics of such models has been deeply used in several network and computer science related solutions. The first and more direct application involves flooding protocols: The information is propagated in a manner rather similar to the way a viral infection spreads in a biological population. Demers et al. [5] firstly recognized the power of these protocols, and since that moment many broadcasting and flooding protocols strongly rooted on those assumptions have been proposed. A comparison of them can be found in [3]. Other approaches use epidemiological model to analyze virus spreading in wireless sensor networks [6], [7].

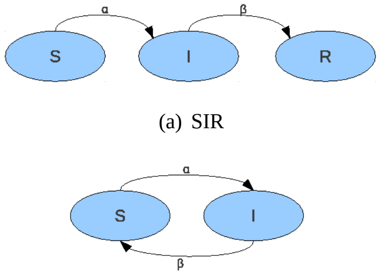
The previously cited papers focus on information spreading, in particular on either information broadcasting or flooding. However, we are not interested in providing the whole network with a given information: we would assure the information survivability in UWSN using the less possible waste of energy. Data-centric storage protocols study a similar problem using *network coding*. In this case information and coding theory is involved with the intent to combine many packets together for transmission [8], [9]. These techniques are more performing than simple data replication when bandwidth and sensor buffers are limited, but they introduce a time delay and a computational overhead. Further, it should be taken into account that bandwidth requirement is not such a limiting issue in event driven networks, should data be generated only sporadically. Therefore, in our settings it is preferable to design a replication scheme that allows the careful selection of the replication rate assuring at the same time data survivability and limited power consumption and bandwidth usage.

UWSNs have been introduced by Di Pietro et Al. [1]. This work has been then extended in [10] to face an adversary that indiscriminately erases all sensor data, and then in [11] cryptographic techniques that prevent the adversary from recognizing data that it aims to erase have been introduced. Sensor cooperation to achieve self-healing in stationary UWSNs has been explored in [12] and [13]. Almost all these works require sensors with some cryptographic ability. Instead, we propose a straightforward non-cryptographic technique that use a simple replication approach without assuming such a prerequisite. Chakrabarti et Al. [14], assuming link and sensor fault probabilities, focus on the information survival threshold in sensors and P2P networks. They analyze the conditions that lead to a quick spread or quick extinction of the datum, but the authors neither consider the presence of an attacker, not take into account power consumption. Finally, note that a detailed characterization of the SIS model is provided in [15].

III. Epidemic Models

In biology, when studying an infectious disease at the population scale there are basically two approaches: the stochastic and the deterministic one. Stochastic models can accurately describe fluctuations, chance variation in risks of exposure, and other factors, but they may become very complex and laborious to set up. In general, it is hardly possible to explain the dynamic of the disease. Instead, deterministic models describe in detail, on the average, the dynamic of the disease at the population scale, fitting very large populations. We will focus on deterministic models.

Generally, in deterministic epidemic models, a population of n individuals is partitioned into several compartments, and the spreading of the disease is taken into consideration. Given the transition probabilities between any two compartments, it is possible to predict the evolution of these systems as times go by. In the following, we introduce two of these models, that are illustrated in Figure 1. In each instant of time t, we will use $X(t)$ to indicate the number of individuals that are in a compartment X, while with $x(t) = X(t)/n$ we will indicate the quantity representing the fraction of individuals in that compartment.



(a) SIR

(b) SIS

Figure 1. Epidemic models.

A. SIR

The SIR model [16] is represented in Figure 1(a). It assumes three compartments named Susceptibles (S), Infected (I) and Recovered (R). A susceptible individual becomes infected with a certain probability (α) if it comes in contact with an infected individual, while an infected individual could recover with probability β. Therefore, the fraction of individuals that can contract the disease at time t is proportional to $\alpha i(t)s(t)$, while the fraction of individuals that becomes recovered at time t is proportional to $\beta i(t)$. Other transitions between compartments are not possible. Thus, the evolution of the system is completely described by the following three differential equations:

$$s'(t) = -\alpha s(t)i(t) \tag{1}$$

$$i'(t) = \alpha s(t)i(t) - \beta i(t) \tag{2}$$

$$r'(t) = \beta i(t) \tag{3}$$

This system is non-linear, and it does not admit a generic analytic solution. However, significant results can be derived analytically. Note that $s'(t)+i'(t)+r'(t) = 0$, and therefore $S(t) + I(t) + R(t) = n$. By dividing the first differential equation by the third, separating the variables and integrating we get:

$$s(t) = s(0)e^{-\frac{\alpha}{\beta}(r(t)-r(0))}$$

The value $\frac{\alpha}{\beta}$ is the *basic reproduction number* and it is often indicated with R_0. It plays a crucial role in the dynamic of the system. Indeed, it holds true that if $\frac{\alpha}{\beta} > \frac{1}{s(0)}$ then $i'(0) > 0$, and there will be an epidemic outbreak with an increase in the number of the infectious. The Basic Reproduction Number is a metric that is useful also in other models to determine whether or not an infectious disease will spread through a population. In general terms, it is the mean number of secondary cases a typical single infected case will cause in a population with no immunity to the disease in the absence of interventions to control the infection.

B. SIS

Another well known epidemic model is the SIS [4]. It assumes only two compartments named Susceptibles (S) and Infected (I). Transitions between these compartments are represented in Figure 1(b). An individual that is susceptible to a disease becomes infected with a certain probability (α), while an infected individual immediately becomes susceptible once (and *if*) it is cured of an infection (which happens with probability β). Note that a healthy individual can contract a disease only if it is in contact with a sick one. Thus, the evolution of this system is completely described by the following two differential equations:

$$i'(t) = \alpha s(t)i(t) - \beta i(t) \tag{4}$$

$$s'(t) = \beta i(t) - \alpha s(t)i(t) \tag{5}$$

When considering a population that does not change during time, $s'(t) = 1 - i'(t)$. Therefore, equations 4 and 5 are not independent, and to study their behavior it is enough to study only one of them. Equation 4 has the following general solution:

$$i(t) = -\frac{(\alpha - \beta)}{e^{t(\beta-\alpha)+c(\alpha-\beta)} - \alpha} \tag{6}$$

where c is a constant that depends on the initial conditions. Therefore, using Equation 6, it is possible to predict the number of sick individuals at time t, and thereby the number of healthy individuals.

IV. Modeling the Information Spread

A. Network, Adversary, and Sink models

We consider an Unattended WSN composed by n sensors. A secure routing protocol allows to exchange message between all the pairs of sensors belonging to the network. To simplify the analysis, we consider the survivability of a single datum initially sensed by one or a little subset of sensors. The evolution time is partitioned in rounds: in each round both the sensors than the attacker play their game. Sensors will use a pure replication approach to preserve the information, while the attacker will try to compromise them with the final target to completely erase the information from the network before the sink collects it. We will indicate with $S(t)$ the number of sensors that do not possess the datum at time t, and with $I(t)$ the number of sensors possessing it. Instead, with $R(t)$ we will indicate the number of sensors that have been destroyed by the attacker at time t. With the notation $s(t)$, $i(t)$ or $r(t)$ we will indicate the fraction of nodes belonging to the corresponding sets, that is: $s(t) = \frac{S(t)}{n}$, $i(t) = \frac{I(t)}{n}$, $r(t) = \frac{R(t)}{n}$. In this paper, we will take into account two kind of attackers: $\mathtt{ADV_{simple}}$ that is able to destroy sensors, and $\mathtt{ADV_{stealth}}$ that is able to erase the datum without destroying the sensor, and without changing its behavior. We will see that the system composed by n sensors and $\mathtt{ADV_{simple}}$ can be modelled with the SIR. When $\mathtt{ADV_{simple}}$ is replaced with $\mathtt{ADV_{stealth}}$, the system can be modeled with the SIS model. In the following, when the context is clear, we write i, s or r instead of $i(t)$, $s(t)$ or $r(t)$.

UWSN are characterized by the presence of an intermittent trusted collection point, also called *intermittent sink*. we will consider an intermittent sink that in each round is able to contact and check out only a subset of all the sensors belonging to the network. More specifically, in each round it collects the datum from each node with probability γ.

B. *Sensors model*

The behavior of the nodes belonging to the UWSN is simple: Data is transmitted by the subset of sensors possessing it, to other sensors randomly selected among those belonging to the network. In particular, each sensor that currently stores the datum will transmit it with probability $\frac{\alpha}{n}$. The following theorem shows that this behavior corresponds to the infective process (with transition rate α) used in the SIR and in the SIS epidemic models.

Theorem 4.1: Given a wireless sensor network composed by n sensor, if the fraction of sensors that possess a datum is equal to i, and if each sensor forward the datum with probability $\frac{\alpha}{n}$, the value $si\alpha$ is a good approximation of the probability that the datum reaches a sensor that do not possess it, where s is the fraction of sensors that do dot possess the datum.

Proof: A sensor $\mathcal{N}_a$ obtains the information during round t if it did not possess it before, and if at least one of its neighbors forwarded the datum to it during that round. Let us indicate with $\Pr[A]$ the latter probability. It holds true that $\Pr[A] = 1 - \Pr[B]$, where B is the event "no sensor sent the datum to $\mathcal{N}_a$". Since there are in sensors that currently possess the datum, $\Pr[B] = \left(1 - \frac{\alpha}{n}\right)^{in}$, and therefore $\Pr[A] = \left(1 - \left(1 - \frac{\alpha}{n}\right)^{in}\right)$. The probability that $\mathcal{N}_a$ does not possess the datum is simply s. So, the probability that the datum reaches a sensor that do not possess it is

$$s * \left(1 - \left(1 - \frac{\alpha}{n}\right)^{in}\right) \tag{7}$$

Now note that $\frac{\alpha}{n}$ is a real number close to 0, indeed α is contained in the interval $[0, 1]$, while $n >> 1$. Using the binomial approximation, Equation 7 is equal to: $s * \left(1 - \left(1 - in\frac{\alpha}{n}\right)\right) = s * i * \alpha$, concluding the proof. ■

V. Using Epidemic Models in UWSNs

We will now show how to assure the information survivability in an UWSN leveraging on the epidemic models introduced in Section III. Depending on the type of attacker, the UWSN scenario will be modelled either with the SIR or with the SIS.

A. *SIR in Unattended Wireless Sensor Networks*

We now consider the sensor network model described in Section IV-A, in presence of an the $\texttt{ADV}_{\texttt{simple}}$ attacker: It is able to individuate the sensors containing the target information, and to destroy each of them with a certain probability β. In each round t, we will indicate with $R(t)$ the number of sensors that have been destroyed by the attacker until round t. Theorem 4.1 proves that if each sensor forwards the information with probability $\frac{\alpha}{n}$, this process corresponds to an epidemic contagion with infective rate equal to α. Further, sensors can be destroyed by the attacker with probability βi, indeed β is the probability that the attacker destroys a sensor, and i is the number of sensors possessing the information. Hence, the described system (composed by n sensors and one adversary that behaves as above) can be modelled with the SIR epidemic model (equations 1 to 3). Here, the datum corresponds to a disease. Each healthy subject (sensor) can contract the disease (the datum) from a sick individual (a sensor that already has the datum) with a certain probability α. The adversary, instead, corresponds to the process of recovering from the disease (or to pass-away). A recovered subject (that is, a sensor that has been destroyed in a previous round) cannot re-contract the same disease (that is, re-acquire the datum). Figure 2 compares the results of a simulation executed in a network composed by 100 sensors, with the forecasting of the SIR. The line indicated with "Simulator Mean" represents the mean over 100 measurements, where α is set equal to 0.6, β to 0.5, and $I(0) = 10$. It can be seen that our model exactly matches the SIR prediction.

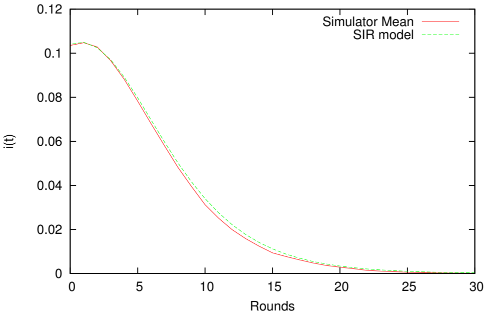


Figure 2. SIR: Comparing the SIR model forecasting with our experimental results. Here, $\alpha = 0.605$, $\beta = 0.5$, $n = 100$ and $I(0) = 10$.

Since the SIR model well describes this scenario, it is possible to use it in order to forecast the survivability of the datum in each round t. To assess this, we will introduce an analysis of the conditions that can produce an information outbreak with an increase in the number of the sensors storing the information. To study the conditions that can produce an information outbreak, it is needed to study the sign of $i'(t)$ when $t = 0$. The expression $i'(0)$ can be written as $i'(0) = i(0)\alpha(s(0) - \frac{\beta}{\alpha})$, and since $i(0)$ and α are greater than or equal to 0, the sign depends on the value $s(0) - \frac{\beta}{\alpha}$. If $s(0) = \frac{n-1}{n}$, that is only one sensor out of n posses the information at time $t = 0$, then we will have an information outbreak only when $\alpha > \frac{\beta n}{n-1}$. This result can be used to set the replication rate once we forecast the maximum compromising power β of an adversary.

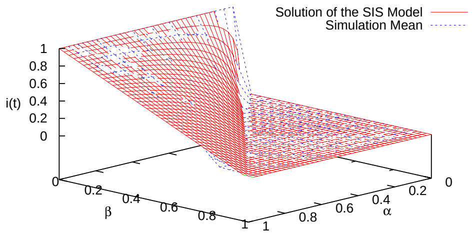


Figure 3. SIS: Comparing the SIS model forecasting with our experimental results.

B. *SIS in Unattended Wireless Sensor Networks*

Considering the same network described in Section IV-A, let us now to take into account the stealthy attacker $\texttt{ADV}_{\texttt{stealth}}$: It will erase all the data a sensor stores, but without changing its behavior neither destroying it. Since it does not change the behavior of the sensors, when a node is attacked it will loose the information, but in the subsequent steps it can re-acquire it. The described system (composed by n sensors and one adversary that behaves as above) can be modeled with the SIS epidemic model (equations 4 and 5). Indeed, Theorem 4.1 assures that the transmission corresponds to the infection process of the SIS epidemic model. The adversary, instead, corresponds to the process of healing from the disease. A healed subject (that is, a sensor that has been in the compromised status in a previous round) can then re-contract the same disease (that is, re-acquire the datum). In Figure 3, we compared the SIS model forecasting (Equation 6), with the result of a simulation over a network of $n = 100$ sensors.

In the SIS model there are two equilibrium points, called *steady states*. When a steady state is reached, the rate of sensors possessing the information will remain indefinitely constant. We will indicate these two steady states with STEADY_0 and STEADY_1. This states are reached when $i'(t) = 0$. It can be proved that STEADY_0 is reached when $i(t) = 0$, while STEADY_1 is reached when $i(t) = 1 - \frac{\beta}{\alpha}$. Further, it can be proved that when $\alpha > \beta$ the system will reach STEADY_1. Note that this aspect is relevant from the point of view of the information insurance because it means that the information will became endemic: The network will never loose it.

VI. Problems of the deterministic modelling

Epidemic models can be used to forecast the behavior of an UWSN. Since these models can be described with differential equations that can be solved (either analytically or numerically), several observations about the set up of a network can be made. For example, we showed that it is possible to study the conditions that have to be satisfied to assure the information survivability. However, one aspect that must be taken into consideration is the minimization of the energy consumption. In UWSNs, like in WSNs, it is important to minimize the communications among the sensors. Therefore, it is important to study the conditions that can assure the information survivability, and at the same time the minimal power consumption.

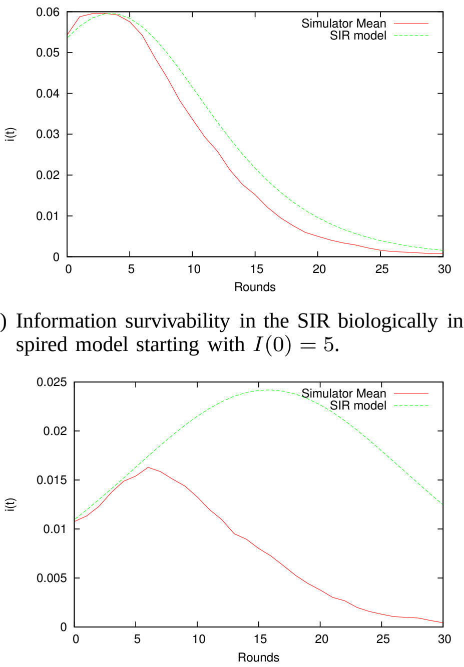
In both the epidemic models we analyzed, saving energy corresponds to select the minimal α, once figured out which is the the maximum compromising power of the adversary. However, not always this is the best choice: Epidemic models do not take into account "unlikely" events. Let us consider for example the SIS model. After the first round, STEADY_0 is an "absorbing" state: The transition probability to move away from the state STEADY_0 is 0. Indeed, it is possible to move away from it only in the first round, that is $t = 0$ (only in this round the datum is generated). Since we want to minimize α, we will use a value greater than β (but very close to it). The system will then reach steady state STEADY_1, where $i(t) = \left(1 - \frac{\beta}{\alpha}\right)$. With these settings, $i(t)$ will be close to 0 in each round t. Unfortunately, when $i(t)$ is close to 0, a statistical fluctuation can force the system to enter STEADY_0, and the prediction of endemicity (that is, the assurance that information will survive) will be violated. Hence, it is important to further investigate the problem and to give probabilistically sound bounds that assure the information survivability, even when α is minimized.

Note that the SIR model has a similar problem when $i(t)$ is close to 0. It is highlighted in Figure VI. In particular, Figure 4(a) illustrates the prediction of the SIR model compared with the results of our simulator when $I(0) = 5$. It can be seen that the prediction of the model and the results of the simulations are slightly different, and unfortunately the results of the simulations are worse than the SIR prediction. Figure 4(b) shows that when $S(0) = 1$ this phenomenon is even more relevant. Also in this case the problem is that "unlikely" events can force the system to loose forever the datum. A possible solution can be for example to use a higher α for the first l replication steps in order to assure to reach a status where $S(l)$ is large enough with high probability.

VII. Conclusion

We modeled the information survivability in UWSNs using an approach inspired by the epidemic domain. However, we also pointed out that these approaches do not take into account "unlikely" events that can induce the loss of the datum. In particular, we investigated two epidemic models to derive the conditions that can assure the survivability of the datum in presence of two different types of attackers—introduced in this paper. We showed that the two selected epidemic models well adapt to the UWSN scenario.

The approach introduced in this paper to model information survivability in UWSNs paves the way for further investigations in the UWSN domain. For instance, assessing bounds on the probability of the events that can compromise the



(a) Information survivability in the SIR biologically inspired model starting with $I(0) = 5$.

(b) Information survivability in the SIR biologically inspired model starting with $I(0) = 1$.

Figure 4. SIR in UWSNs: Problems that can arise without selecting the appropriate parameters.

information survivability, while taking into consideration energy and quality of service issues.

Acknowledgments

The authors would like to thank Riccardo Mariani for his contribution to numerical simulations.
This work has been partially supported by: 1) the EU FP7-ICT project NESSoS (Network of Excellence on Engineering Secure Future Internet Software Services and Systems) under the grant agreement n.256980; and, 2) the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme - European Commission - Directorate-General Home Affairs, under the ExTraBIRE project, HOME/2009/CIPS/AG/C2-065.

References

[1] R. Di Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, "Catch Me (If You Can): Data Survival in Unattended Sensor Networks," *2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 185–194, Mar. 2008.

[2] R. Di Pietro, G. Oligeri, C. Soriente, and G. Tsudik, "Securing mobile unattended wsns against a mobile adversary," *Reliable Distributed Systems, IEEE Symposium on*, pp. 11–20, 2010.

[3] M. Akdere, C. Bilgin, O. Gerdaneri, I. Korpeoglu, O. Ulusoy, and U. Cetintemel, "A comparison of epidemic algorithms in wireless sensor networks," *Computer Communications*, vol. 29, no. 13-14, pp. 2450–2457, Aug. 2006.

[4] W. O. Kermack and A. G. Mckendrick, "A Contribution to the Mathematical Theory of Epidemics," *Royal Society of London Proceedings Series A*, vol. 115, pp. 700–721, 1927.

[5] 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*. ACM, 1987, pp. 1–12.

[6] S. Tang and B. L. Mark, "Analysis of virus spread in wireless sensor networks: An epidemic model," *2009 7th International Workshop on Design of Reliable Communication Networks*, pp. 86–91, Oct. 2009.

[7] P. De, Y. Liu, and S. K. Das, "Modeling Node Compromise Spread in Wireless Sensor Networks Using Epidemic Theory," in *WOWMOM '06: Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*. Washington, DC, USA: IEEE Computer Society, 2006, pp. 237–243.

[8] Y. Lin, B. Li, and B. Liang, "Stochastic analysis of network coding in epidemic routing," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 5, pp. 794–808, June 2008.

[9] W. Ren, J. Zhao, and Y. Ren, "Network coding based dependable and efficient data survival in unattended wireless sensor networks," *JCM*, vol. 4, no. 11, pp. 894–901, 2009.

[10] R. Di Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, "Data Security in Unattended Wireless Sensor Networks," *IEEE Transactions on Computers*, vol. 58, no. 11, pp. 1500–1511, 2009.

[11] ——, "Playing hide-and-seek with a focused mobile adversary in unattended wireless sensor networks," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1463–1475, Nov. 2009.

[12] R. Di Pietro, D. Ma, C. Soriente, and G. Tsudik, "POSH: Proactive co-Operative Self-Healing in Unattended Wireless Sensor Networks," in *SRDS '08: Proceedings of the 2008 Symposium on Reliable Distributed Systems*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 185–194.

[13] D. Ma and G. Tsudik, "DISH: Distributed Self-Healing," in *SSS '08: Proceedings of the 10th International Symposium on Stabilization, Safety, and Security of Distributed Systems*. Detroit, MI: Springer-Verlag, 2008, pp. 47–62.

[14] D. Chakrabarti, J. Leskovec, C. Faloutsos, S. Madden, C. Guestrin, and M. Faloutsos, "Information Survival Threshold in Sensor and P2P Networks," *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, pp. 1316–1324, May 2007.

[15] R. Di Pietro and N. V. Verde, "Epidemic data survivability in unattended wireless sensor networks," in *The Fourth ACM Conference on Wireless Network Security (Wisec'11), to appear*.

[16] E. Allman and J. Rhodes, *Mathematical Models in Biology: An Introduction*. Cambridge University Press, 2004.