An Epidemiological Approach for Mobile Ad-Hoc Networks Monitoring

Christophe Guyeux, Abdallah Makhoul, and Jacques Bahi
Femto-St Institute, UMR 6174 CNRS
Université de Bourgogne Franche-Comté, France
Email: {first}.{last}@femto-st.fr

***Abstract*—MANETS are vulnerable to many types of attacks. Moreover, many challenges arise in the MANET management, such as dynamic network topology, limited bandwidth, storage capacity, battery life and processing power. In order to ensure high network performance, an important function of network management is monitoring. It consists in observing the operational states of the connected mobile nodes and controlling the application quality of service and prevent attacks. Indeed, malicious participants may disrupt the system through altering the collected data, reporting false measurements, defining new management policies or flooding f alse a larms. I n t his paper, an epidemic model is developed to ensure an efficient MANET monitoring. It will be useful in various contexts, to provide for instance design parameters of the MANET such that the number of malicious nodes always remains under control. Theoretical modeling and analysis of various situations are then provided, and simulations results on real case scenario are proposed.**

***Keywords*—Mobile ad hoc networks; Epidemiological approach; Monitoring model; Security**.

I. Introduction

A Mobile Ad hoc NETwork (MANET) is defined a s an autonomous and infrastructure less system of mobile devices, such as laptop, mobile phones,Personal Digital Assistant (PDA), etc. [1] [2] which can be connected everywhere [3] [4] [5] [6]. These devices can cooperate to maintain this temporary network and to provide services like routing, service discovery, and other application services. Some of the challenges that face MANETs are dynamic network topology, undefined geographical coverage area, limited resources (battery power, bandwidth, central processing unit (CPU) and storage space), communication overhead, security, mobility, scalability, and so on [7] [8] [9] [10]. Considering these specific c onstraints, a mechanism of self monitoring must be implemented to control the network state.

Monitoring of MANET consists in observing the operational states of the connected mobile nodes, controlling the application quality of service and preventing attacks. Monitoring can further be concerned with malicious attacks prevention. This monitoring is achieved by a subset of mobile nodes (called monitors) which are elected according to several predefined parameters [11]. Each monitor performs its assigned tasks (collect and process data) and, at the same time, is responsible for controlling and monitoring a subset of mobile nodes in its area called the monitored nodes.

In this article, we propose to determine the optimal parameters of a the network monitoring by means of epidemiological models. The total number of sensors is divided by compartment, according to their intrinsic nature: monitored, monitoring, selfish, or malicious. Furthermore, various rates define the state modification of a sensor (e.g., from monitoring to malicious after a successful attack) [12] [13]. According to the complexity of the model, which can take under consideration the death rates, any scheduling process, or the discovery of new nodes, the resulted differential system can either be theoretically handled or it can only be observed through numerical simulations. All these situations are presented in this article, whose aim is to illustrate the power of epidemiological modeling in the study of MANET monitoring.

The remainder of the paper is organized as follows. A brief state of the art is presented in the next section. Then, an example of study of a MANET at short timescales is proposed in Section III. Section IV presents some numerical simulations in the most complex situation where monitored, monitoring, selfish, and malicious nodes are present in the network. This article ends by a conclusion section, where the contribution is summarized and intended future work is outlined.

II. Related Work

In the literature, we can find several approaches for MANET monitoring. The aim of these works is to guarantee an efficient quality of service of the network in spite of the presence of some anomalies and in the presence of malicious or selfish nodes [14].

Liu et al. [15] propose an epidemic model for rechargeable wireless sensor networks. This model is based on pulse charging and aims to model the low and normal energy in each periodic pulse point. In [16], the authors propose a secure multi-casting in order to ensure data secret transmission between the manager, the cluster heads, and the agents. Thus, the exchanged data must be encrypted with timeliness information and with a digital signature. Moreover, a level-based access control model is implemented to protect the monitoring data from unauthorized access. However, the authors do not specify how the manager generates the security level of each node. In [17], the authors propose a probabilistic scheme in order to enhance the reliability of monitoring by

 ISBN: 978-1-68558-017-9

excluding the dishonest managed nodes that provide unreal data management from the data collection. Nevertheless, the scheme effectiveness depends on the exchanged measurements correctness [18]. Furthermore, the authors do not take into account the managers malicious behavior.

A survivable monitoring that allows a set of nodes called domain nodes to monitor the behavior of visitors when they join their domains, is presented in [19]. It supposes that the supervisor is reliable and trusted and that the domain nodes are too. In [20], the authors propose to assess the selfish behaviors of each monitored node regarding its co-operations in forwarding others packets. However, it is a passive monitoring. In addition, they do not take into account the monitoring units malicious and selfish behaviors.

The authors of [21] propose to authenticate mobile nodes in order to detect intrusion. Thus, they use a non-interactive zero knowledge technique to determine a set of nodes having access to specific applications or services in MANET. Among these authorized nodes, only those with the highest battery life can play the role of monitors. However, the authors do not take into account the monitors malicious or selfish behaviors. Finally, in [22], the authors aim to detect the inappropriate behaviors of mobile nodes for ensuring efficient routing. In fact, they propose to add three components: a monitor, a reputation system, and a path manager, to the DSR (Dynamic Source Routing) routing protocol functionality.

All these limitations in the related works provide us with the motivation to propose a new monitoring scheme based on epidemiological modeling [23] [24]. Indeed, in this paper, we consider a monitoring approach as efficient if it aims to perform correctly and legally the monitoring tasks in spite of the presence of some anomalies (mobility or the failure of a monitor, unavailability of routes between monitors and some monitored nodes, etc.) and in the presence of malicious and selfish nodes as well. The theoretical study will encompass short and large timescales, while a more complete model will be investigated by means of numerical simulations.

III. Studying the MANET at short timescales

Let us firstly consider 3 types of sensors:

- monitored $S(t)$,
- monitoring $I(t)$,
- malicious $R(t)$.

Malicious nodes attack the monitors and make them unable to do their work. These monitors, once attacked, become in turn malicious. The adversary goal is to corrupt all the monitor nodes ($I(t) \longrightarrow 0$ when $t \to +\infty$). Conversely, the user wants the guarantee that, at each time, at least one of these monitors is available for network surveillance ($\forall t, I(t) > 0$).

We suppose in this article that attacks need contacts to be performed (*i.e.*, a monitor must be within the transmission range of a malicious node), and we denote by β the rate of successful attacks per contact. It is therefore, a rate of "effective contacts" between monitor and malicious nodes, in terms of epidemiological models. When such an effective contact occurs, the considered sensor moves from the I compartment (monitoring) to the R (malicious) one.

Furthermore, let us denote by α the rate, constant over time, of sensors moving from the "monitored" state to the "monitoring" one. In practice, this rate depends on numerous parameters: node reputation, their capacity, and their ability (CPU, memory, mobility, energy, etc.). Let us remark that, if the number of neighbors (that is, the degree of the node in the connectivity graph) can be part of these parameters, most of the times it is only a secondary factor according to the literature.

We denote by $N = S(t) + I(t) + R(t)$ the total number of sensors. It will firstly be supposed to be constant, as we will consider first the evolution of the network on small timescales: the energy consumption (and the node failure due to an empty battery) is negligible under such assumption. Indeed, the objective at the beginning of this study is to evaluate if it is possible to avoid, on small timescales, that $I(t)$ becomes equal to 0.

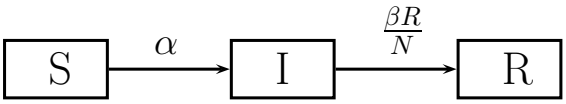


Figure 1: Our first compartmental model

Having the definitions of S, I, and R on the one hand, and the rates α and β on the other hand, we are then left to study the compartmental model depicted in Figure 1. To begin with, let us remark that, in the literature of epidemiological models, susceptible individuals become infected proportionally to their contacts with infected individuals, while infected people become recovered at a rate independent from any contact. In other words, the non-linearity is usually between S and I compartments, leading to the classical SIR model depicted in Figure 2.

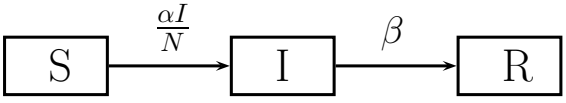


Figure 2: Usual SIR model

Our first model based on the MANETs study is not usual and, until now, it has never been studied in the literature. This remark still remains valid for the more refined models that will be presented later in this article. However, if the differential equations deduced from a compartmental modeling of MANET monitoring are different from the ones usually found with classical models (like the so-called SIR, SIS, SEIS, and so on), their shape is similar enough to consider that existing tools and methods may be applied to them too, in order to resolve them. The model in Figure 1 can be

 ISBN: 978-1-68558-017-9

formulated using differential equations, as follows.

$$\begin{cases} \dot{S} = -\alpha S \\ \dot{I} = \alpha S - \frac{\beta}{N} IR \\ \dot{R} = \frac{\beta}{N} IR \end{cases} \quad (1)$$

As we suppose, in this section, that the total number of sensors is constant over time, then $S(t)$ can be deduced from $I(t)$ and $R(t)$, as follows:

$$S(t) = N - I(t) - R(t).$$

We can thus only consider the two last variables and the two last equations in Eq. (1):

$$\begin{cases} \dot{I} = \alpha(N - I - R) - \frac{\beta}{N} IR \\ \dot{R} = \frac{\beta}{N} IR \end{cases}$$

We can focus now on proportions $\frac{I}{N}$ and $\frac{R}{N}$, which are renamed as I and R, which leads to the normalized equation:

$$\begin{cases} \dot{I} = \alpha(1 - I - R) - \beta IR \\ \dot{R} = \beta IR. \end{cases} \quad (2)$$

Let us remark first that $\dot{R} \geqslant 0$. So, at short timescale such that the energy consumption is negligible, the number of malicious nodes necessarily increases (similarly, in the usual SIR model, the number of susceptible necessarily decreases).

The equilibrium solutions satisfying $\dot{I} = \dot{R} = 0$ are such that:

- either $R = 0$, and so $I = 1$,
- or $I = 0$, and so $R = 1$.

In other words, the two equilibrium solutions of the system are either when all the nodes are monitor ones, or when they all are malicious. Starting in such a configuration, the system will obviously not evolve.

Let us now study the behavior of the network at the neighborhood of these equilibrium points, *i.e.*, when the proportions of monitor I and malicious R nodes are either close to $(1, 0)$ (almost all nodes are monitors) or $(0, 1)$ (almost all nodes are malicious). In order to do so, the system can be linearized. Its Jacobian matrix is equal to:

$$\begin{pmatrix} -\alpha - \beta R & -\alpha - \beta I \\ \beta R & \beta I \end{pmatrix}.$$

At the equilibrium $(1, 0)$, this latter is equal to:

$$\begin{pmatrix} -\alpha & -\alpha - \beta \\ 0 & \beta \end{pmatrix}.$$

This matrix being triangular, its eigenvalues are on the main diagonal: $-\alpha$ and β. α and β being positive, we thus find non null eigenvalues with opposite signs. So, the equilibrium point $(1, 0)$ is a saddle point in the phase diagram of (I, R).

Let us consider now the neighborhood of the point $(0, 1)$. The Jacobian matrix on this equilibrium point is equal to:

$$\begin{pmatrix} -\alpha - \beta & -\alpha \\ \beta & 0 \end{pmatrix}.$$

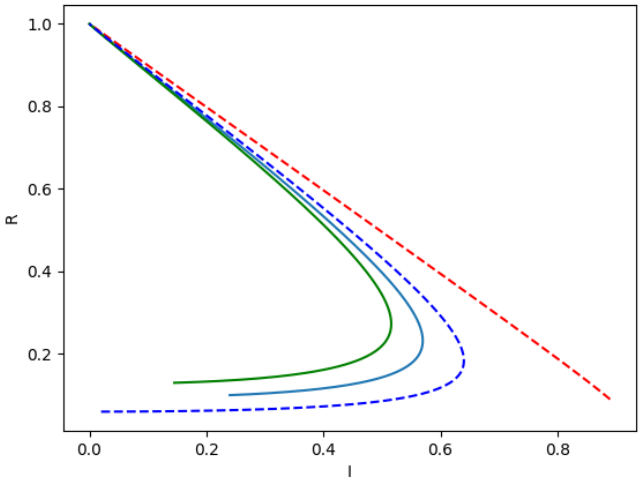


Figure 3: Network behavior (I and R rates) close to the equilibrium position (0,1).

The characteristic polynomial being $X^2 + (\alpha + \beta)X + \alpha\beta$, its two eigenvalues are $-\alpha$ and $-\beta$. Being of the same negative sign, we can conclude that this equilibrium position $(0, 1)$ is stable, see Figure 3. Note that, as $\dot{R} = \beta IR$, we have $\dot{R} \geqslant 0$. So, R can only increase, which explains the shape of the curves in Figure 3.

To sum up, either there is no malicious node at initial time, and so in the absence of energetic considerations, all the monitored nodes eventually become monitoring ones. Or there is at least one malicious node and, over time, all nodes become malicious. Such a description of the MANET behavior is only valid when operations between nodes are negligible when compared to the sensors lifetime.

After having investigated some capabilities of a theoretical study of a MANET described in terms of epidemiological models, we now numerically illustrate various evolutions of the numbers of nodes according to the parameters of the system.

IV. Numerical simulations

We now consider the existence of selfish nodes, that for instance become inactive for the monitoring when their battery is below a given threshold. We consider too the possibility that a monitoring node switches to the monitored state, for example if its battery is below a critical value. Such considerations evoked in the literature lead to the compartment model depicted in Figure 4. This model contains now four compartments, corresponding to the inactive (compartment A), monitored (B), monitoring (C), and malicious (D) nodes. Various parameters can be defined between these four compartments.

- Λ is the rate used to define the integration of new mobile devices within the area, which will populate the

 ISBN: 978-1-68558-017-9

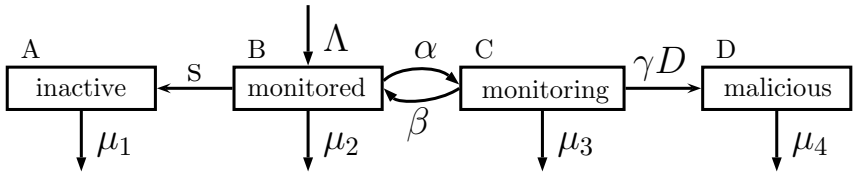


Figure 4: A more global compartmental model for MANET

B compartment (as new devices are first set to monitored mode).

- s is the rate under which some monitored nodes become selfish, and thus stop to participate to the network. This rate can be defined as a proportion of monitored devices that, under a given energy threshold, prefer to preserve themselves instead of the network.
- α is the rate at which monitored nodes start to monitor the network. By doing so, they become more useful for the network, but their activity increases accordingly, leading to a reduced lifetime.
- Conversely, β is the rate on which a monitoring device stops its monitor activity. According to the literature, this may be for a large variety of reasons, encompassing a coverage issue (too many monitors in a given area, or a too small number of devices to monitor), battery level, etc.
- Between C and D compartments, the rate is γD, which is proportional to the number of malicious devices. γ measures the probability of success that a malicious node achieves to convert a monitoring node. Indeed, we consider in this simulation that, in case of a successful attack, the attacked monitoring device becomes a malicious one (but other configurations are possible). As such an attack needs a contact with a malicious node, this rate is proportional to D.
- μ_1, μ_2, μ_3, and μ_4 are the "death" rates associated with the four aforementioned compartments. They are the rates that correspond to the depopulation of each compartment: mobiles that have emptied their batteries or that become deficient stop to be considered in their associated compartment, as they cannot participate anymore to the network life.
- Finally, the activity and the strength of malicious devices are associated to μ_4 and γ, respectively.

Such a compartment model leads to the following nonlinear system of ordinary differential equations:

$$\begin{cases} \dot{A} = sB - \mu_1 A, \\ \dot{B} = \Lambda - sB - \alpha B + \beta C - \mu_2 B, \\ \dot{C} = \alpha B - \beta C - \dfrac{\gamma}{N} DC - \mu_3 C, \\ \dot{D} = \dfrac{\gamma}{N} DC - \mu_4 D. \end{cases}$$

This system can be investigated theoretically, by following an approach similar to what has been introduced in the previous section. However, its larger number of variables and parameters make it harder to study, theoretically speaking. Furthermore, our objective in this article is to show the usefulness of compartment models for MANET studies, and such models can be investigated either theoretically or through numerical simulations. We are then left, in this section, to provide an illustration of the usefulness of numerically simulated compartment models for decision-making aids in complex MANETs.

To reach this goal, we have fully designed a mobile ad-hoc network by using the Python language [25]. Each simulated mobile device belongs initially to one of the four compartments considered in this section, and they change compartments according to the model depicted in Figure 4. For cross validation, the system of ordinary differential equations has been numerically solved too, by using lsoda from the FORTRAN library odepack [26], as it is embedded in SciPy [27]. The obtained results are convergent, and various situations can be emphasized, according to the parameters of the system and to the initial population.

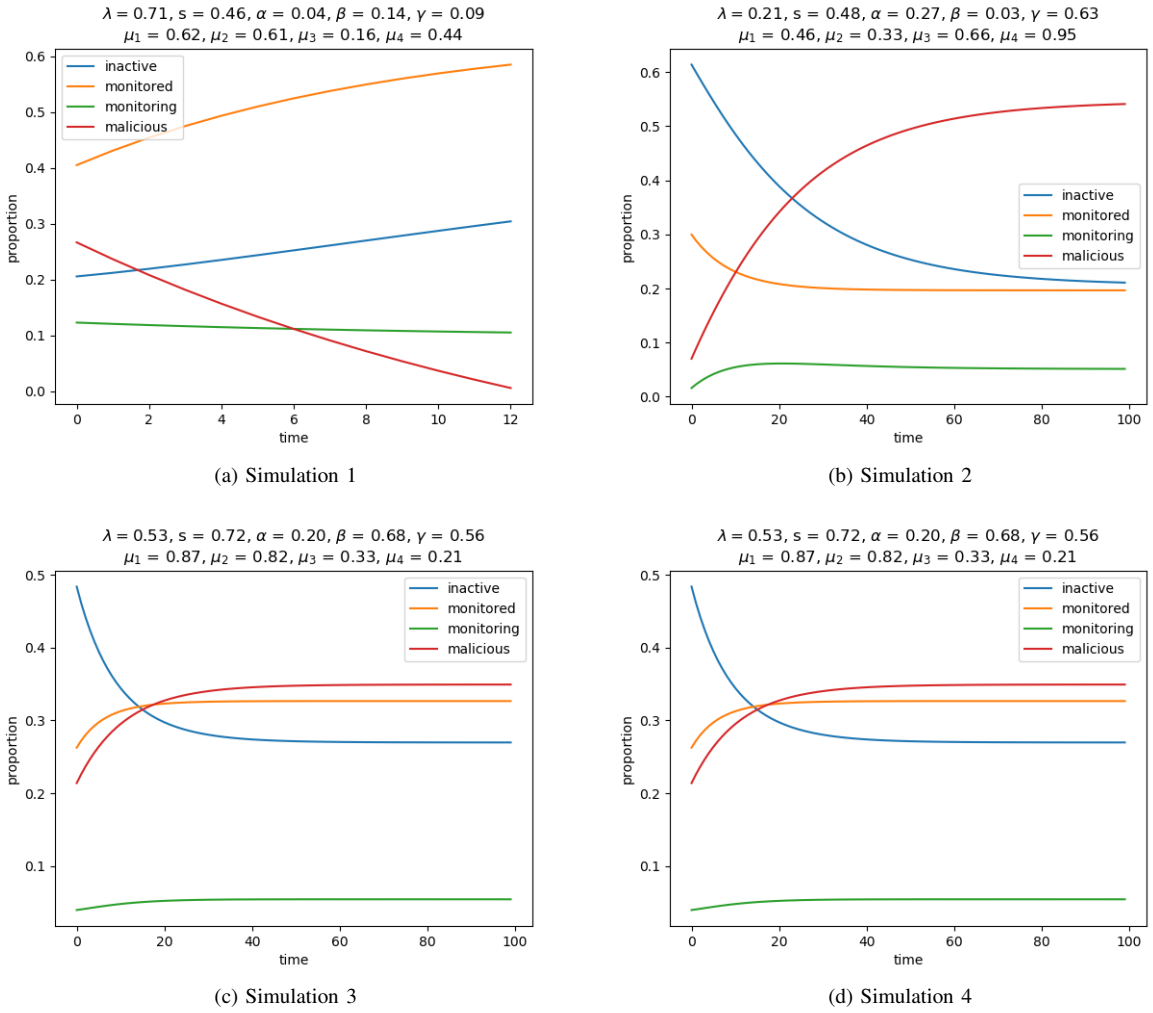
Let us first discuss about the worst case scenarios that are depicted in Figure 5 (for the MANET designer, not for the attackers). First of all, a disastrous situation can be seen in Simulation 1 of Figure 5: the number of malicious devices, which initially were quite low, has increased until reaching the three-quarters of the network. Monitoring and monitored nodes have decreased accordingly. This behavior is mainly due to a very aggressive behavior of the malicious devices, that most of the times achieve their attacks (see the value of the γ parameter). The arrival of new devices, modeled by Λ, is not high enough to counteract the node defections within the MANET. Even though the death rate μ_4 of malicious devices is large here, as such attack performances lead to a large battery consumption, the inactivation of some malicious nodes is totally compensated by the new conversion of monitoring devices to the malicious node.

This behavior is independent from the initial size of the compartment, as can be seen in Simulation 2 of Figure 5. In this simulation, the initial condition is different, but we recover a pronounced increase of malicious nodes over time. This increase is still preserved even if we consider that the malicious device activity has a very important impact on its morbidity (μ_4 is now equal to 0.95).

V. Conclusion and future work

In this article, a short state of the art in the field of MANET monitoring has firstly been presented. This study has then been completed by regarding intermediate timescales, and the evolution of sensor number per compartment has been

 ISBN: 978-1-68558-017-9



(a) Simulation 1

(b) Simulation 2

(c) Simulation 3

(d) Simulation 4

Figure 5: Worst case scenarios

theoretically detailed. Some numerical simulations have finally been presented, in a more complex situation where monitored, monitoring, selfish, and malicious nodes are present in the network.

Other theoretical results can be produced by using this theoretical formulation, using compartments, on the monitoring of a MANET in an hostile environment. For instance, it is possible to compute the maximal number of monitors or of malicious nodes that can be reached for a given set of parameters, and the time needed to reach such an optimum, etc. The results, and the difficulties that can be faced to obtain them, depend both on the compartment model and on parameters. Their exhaustive study, which cannot be completed in an article of limited number of pages, is not the objective of this work. Our intention was just to illustrate the relevance of such a modeling to study the monitoring of MANETs. However, this exhaustive study will be initiated in a couple of forthcoming articles we intend to propose in the future.

ACKNOWLEDGMENT

This work is partially funded by the EIPHI Graduate School (contract “ANR-17-EURE-0002”).

REFERENCES

[1] J. P. Hubaux, L. Buttyan, and S. Capkun, The quest for security in mobile ad hoc networks. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, pp. 146–155, 2001.

[2] M. Ghonge, S. Pramanik, and A. D. Potgantwar, Software defined networking for ad hoc networks, publisher: Springer, 2022.

[3] P. Satyanarayana, M. Vani Pujitha, G. Venkata Subbaiah, and Mugada Srivani. Enhancement of performance parameters in wireless mobile adhoc networks using dsr and cache-modified dsr routing protocols. In *Smart and Intelligent Systems*, pp. 257–267. Springer, 2022.

[4] D. Kanellopoulos and F. Cuomo, Recent developments on mobile ad-hoc networks and vehicular ad-hoc networks. electronics 2021, 10, 364. *Recent Developments on Mobile Ad-Hoc Networks and Vehicular Ad-Hoc Networks*, p. 1, 2021.

[5] J. Azar, A. Makhoul, R. Couturier, and J. Demerjian, Robust IoT time series classification with data compression and deep learning. *Neurocomputing*, 398:222–234, 2020.

 ISBN: 978-1-68558-017-9

[6] A. Makhoul and C. Pham, Dynamic scheduling of cover-sets in randomly deployed wireless video sensor networks for surveillance applications. In *2009 2nd IFIP Wireless Days (WD)*, pp. 1–6, 2009.
[7] M. Chatzidakis and S. Hadjiefthymiades, A trust change detection mechanism in mobile ad-hoc networks. *Computer Communications*, 187:155–163, 2022.
[8] M. Fayaz, G. Mehmood, A. Khan, S. Abbas, and J. Gwak, Counteracting selfish nodes using reputation based system in mobile ad hoc networks. *Electronics*, 11(2):185, 2022.
[9] H. Harb, A. Makhoul, and C. Abou Jaoude, A real-time massive data processing technique for densely distributed sensor networks. *IEEE Access*, 6:56551–56561, 2018.
[10] H. Harb, A. Makhoul, R. Couturier, and M. Medlej, Atp: An aggregation and transmission protocol for conserving energy in periodic sensor networks. In *2015 IEEE 24th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp. 134–139, 2015.
[11] N. Battat, H. Seba, and H. Kheddouci, Monitoring in mobile ad hoc networks: A survey. *Computer Networks*, 69:82–100, 2014.
[12] J. Bahi, C. Guyeux, and A. Makhoul, Secure data aggregation in wireless sensor networks: Homomorphism versus watermarking approach. In Jun Zheng, David Simplot-Ryl, and Victor C. M. Leung, editors, *Ad Hoc Networks*, pp. 344–358, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.
[13] A. Makhoul, R. Saadi, and C. Pham, Risk management in intrusion detection applications with wireless video sensor networks. In *IEEE WCNC*, vol. 182, p. 10. Sydney, Australia, 2010.
[14] J. Bahi, C. Guyeux, A. Makhoul, and C. Pham. Low cost monitoring and intruders detection using wireless video sensor networks. *International Journal of Distributed Sensor Networks*, 2012, November 2012.
[15] G. Liu, K. Su, F. Hong, X. Zhong, Z. Liang, X. Wu, and Z. Huang, A novel epidemic model base on pulse charging in wireless rechargeable sensor networks. *Entropy*, 24(2), 2022.
[16] W. Chen, N. Jain, and S. Singh, Anmp: Ad hoc network man-agement protocol. *IEEE Journal on selected areas in communications*, 17(8):1506–1531, 1999.
[17] R. Badonnel, R. State, and O. Festor, Probabilistic Management of Ad-Hoc Networks. In *NOMS*, pages 339–350, Vancouver, Canada, 2006.
[18] Remi Badonnel, Radu State, and Olivier Festor. Management of ad-hoc networks. In *Handbook of Network and System Administration*, pages 331–360. Elsevier, 2008.
[19] G. Ateniese, C. Riley, and C. Scheideler, Survivable Monitoring in Dynamic Networks. *IEEE Transactions on Mobile Computing*, 5:33–47, Sept. 2006.
[20] H. Kazemi, G. C. Hadjichristofi, and L. A. Dasilva. MMAN - a monitor for mobile ad hoc networks: design, implementation, and experimental evaluation. In *Mobile Computing and Networking*, pp. 57–64, 2008.
[21] M. K. Rafsanjani and A. Movaghar, Identifying Monitoring Nodes with Selection of Authorized Nodes in MANET. *World Applied Sciences Journal*, 4, 2008.
[22] K. Gopalakrishnan and V. R. Uthariaraj, Neighborhood Monitoring Based Collaborative Alert Mechanism to Thwart the Misbehaving Nodes in Mobile Ad Hoc Networks. *European Journal of Scientific Research*, 57(3):411–425, 2011.
[23] A. Makhoul, C. Guyeux, M. Hakem, and J. Bahi, Using an epidemiological approach to maximize data survival in the internet of things. *ACM Transactions on Internet Technology (TOIT)*, 16(1), February 2016.
[24] J. Bahi, C. Guyeux, M. Hakem, and A. Makhoul, Epidemiological approach for data survivability in unattended wireless sensor networks. *Journal of Network and Computer Applications*, 46, November 2014.
[25] G. Rossum, Python reference manual. Technical report, Amsterdam, The Netherlands, 1995.
[26] A. C. Hindmarsh, ODEPACK, a systematized collection of ODE solvers. In R. S. Stepleman, editor, *Scientific Computing*, pp. 55–64, Amsterdam, 1983. North-Holland.
[27] E. Jones et al., SciPy: Open source scientific tools for Python, 2001–. [Online; accessed July 2022].

 ISBN: 978-1-68558-017-9