Fault Monitoring in Ad-Hoc Networks based on Information Theory

Remi Badonnel, Radu State, and Olivier Festor

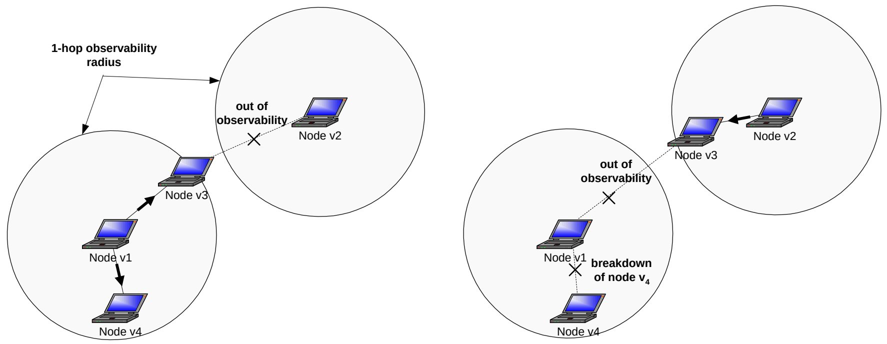
MADYNES Research Team
LORIA-INRIA Lorraine
Campus Scientifique - BP 239
54600 Villers-les-Nancy Cedex, France
{badonnel, state, festor}@loria.fr

Abstract. Fault detection is a well-known issue in fixed wired networks. Ad-hoc networks provide new challenges towards detecting network failures: the detection task may be hindered by the impossibility to observe a given node. We propose in this paper to monitor the intermittence of network nodes in order to infer network failures. Intermittence can be caused in ad-hoc networks by benign causes due to node mobility and to time-limited out of reachability situations. Abnormal intermittence is however due to faults or malicious network activities. This paper shows how information theoretic measures can identify abnormal intermittence over the routing layer, and proposes a lightweight and distributed intermittence monitoring scheme including several fault detection methods.

Keywords: Ad-Hoc Networks, Network Monitoring, Fault Management

1 Introduction

Mobile ad-hoc networks [1] are self-configuring networks spontaneously deployed from a set of mobile devices, where a device can interact as a router to forward packets on behalf of the other devices. Our paper addresses the issue of monitoring ad-hoc networks in order to detect faulty behavior. Faulty behavior and intermittence are closely related in ad-hoc networks: a node can have a regular intermittence due to mobility and other ad-hoc specifics, while faulty behavior can generate abnormal intermittence behavior. The key issue that we address in this paper is how to differentiate abnormal intermittence from regular intermittence and thus identify faulty nodes from regular non-faulty ones. While fault detection in fixed wired networks is not hindered by the impossibility to observe a given node, ad-hoc networks specifics do provide major challenges with respect to this issue. A node that does not reply to legitimate polling in an fixed network is typically considered as not functional. In ad-hoc networks, observability is a major issue: a node might not be reachable because it is moving and is out of reachability, or because it is not functioning properly (see figure 1). A centralized manager/agent architecture is not viable for ad-hoc networks, because the manager itself might become isolated or resource might become exhausted. Resource



(a) Ad-hoc network in phase 1

(b) Ad-hoc network in phase 2

Fig. 1. Fault detection issues in ad-hoc networks. From the perspective of node v_1, both nodes v_3 and v_4 are operational in a first phase. In a second phase, node v_3 goes beyond direct link-level reachability and node v_4 goes down due to faults. From the perspective of node v_1, these two situations are the same.

consumption due to management is neglected in fixed networks, while the same is of major importance in a landscape where bandwidth and battery lifetime are the key actors. We consider the issue of passive and lightweight monitoring of ad-hoc networks. Monitoring should not generate additional traffic and processing efforts and we thus rely on a passive monitoring approach. We monitor routing level information that is anyway processed by ad-hoc nodes and derive an information theoretic framework [2], where abnormal intermittence can be detected. In order to address the reliability of the monitoring infrastructure, we propose and evaluate several distributed collaborative detection methods. Our approach is centered on a distributed lightweight monitoring scheme, where an entropy derived measure is used to identify abnormal behavior. Our approach is lightweight in the sense that the entropic measure is computed on routing level information which is already available at the node. A distributed and collaborative mechanism is introduced to cope with biased local views.

Our paper is structured as follows : after introducing the monitoring challenges, Section 2 presents our lightweight and distributed monitoring approach for detecting abnormal intermittence of ad-hoc nodes. We briefly overview the routing protocol which serves as an underlying data source in 2.1 and present a failure model for ad-hoc nodes in 2.2. An information theoretic measure for monitoring node intermittence is proposed in 2.3. Several distributed methods of abnormal intermittence detection are described in 2.4 and are evaluated by simulations in Section 3. A survey of related work is given in Section 4. Finally, Section 5 concludes the paper and presents future research efforts.

2 Intermittence Monitoring in Mobile Ad-Hoc Networks

Intermittence in ad-hoc networks is a relative normal condition due to causes that are inherent to such a network: nodes are moving, connectivity might be lost for longer or shorter time-periods and battery life is a well-known issue for this target domain. However, intermittence might have also a different cause related to abnormal ad-hoc behavior, where:

- Failures due to miss-configuration and errors at the physical layer might generate an atypical behavior, where nodes will appear intermittent although from a mobility point of view they did not change significantly,
- Routing failures can be encountered when the routing process is affected by voluntary activity [3], malicious activity (attacks against the routing plane), errors in its configuration or at the protocol stack level,
- Abnormal mobility. While normal mobility is difficult to define, in some specific target deployment (for instance military applications), unpredicted mobility patterns can seriously impact the network resilience and service level.

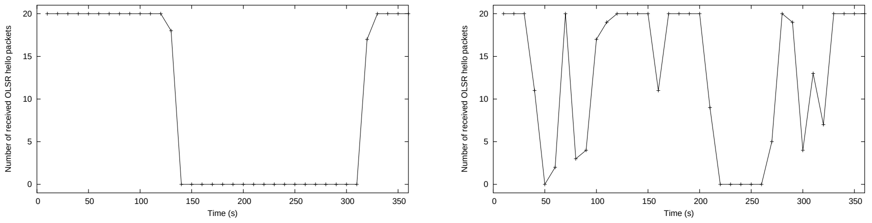
In this paper, we analyze the behavior of intermittent ad-hoc nodes and propose an entropy-based approach for monitoring the routing plane and detecting abnormal intermittent nodes.

2.1 OLSR Routing Protocol Beaconing

The optimized link state routing protocol (OLSR) [4] is a standardized proactive routing protocol that optimizes the pure link state routing algorithms to cope with the requirements of mobile ad-hoc networks. As in a pure link state algorithm, each node determines the list of direct-connected neighbor nodes by accomplishing link sensing through periodic emission of beaconing hello messages. We propose to monitor the routing protocol by analyzing the distribution of hello packets received by each node during the beaconing operation. This is done in order to detect abnormal intermittent ad-hoc nodes. We assume a mobile ad-hoc network as a set of n mobile nodes $V = \{v_1, v_2, ..., v_n\}$ moving in a given surface during a time period T. The time period T is split in k measurement interval $[t_l, t_{l+1}]$ with $t_l = l \times \frac{T}{k}$ for an integer $l \in [0, k]$. During the OLSR beaconing, each node $v_i \in V$ can receive hello packets from the other network nodes located at one hop. The number of beaconing hello packets received by a node v_i from a node v_j is noted X_{v_i,v_j} and can be considered as a random variable $X_{v_i,v_j}(l) : [0, k] \rightarrow [0, b_{max}]$ with l characterizing the interval $[t_l, t_{l+1}]$ and b_{max} the maximal number of hello packets that v_i can receive from v_j. If the hello packets emission interval r is supposed to be homogeneous among network nodes, then X_{v_i,v_j} is bounded by $b_{max} = \frac{1}{r} \times \frac{T}{k}$. This is not a limiting constraint, since the monitoring process can be easily extended to different (per node) r values.

2.2 Ad-hoc node abnormal intermittence

Statement Since monitoring is performed at the routing level, we intent to detect abnormal intermittence due to multiple failure causes such as routing failures, battery problems, physical perturbations and pathological mobility. This monitoring is based on the analysis of how an intermittent node is perceived by a neighbor node or by a set of neighbor nodes. An intuitive idea of intermittence perception by a node can be given by analyzing $X(v_i, v_j)$ values for a network node v_i for different v_j network nodes. Figures 2(a) and 2(b) depict these values respectively for a regular intermittent node and for an abnormal intermittent node. Each figure represents the number of received hello packets $X(v_i, v_j)$ measured (on the y axis) for each time interval $[t_l, t_{l+1}]$ (on the x axis). In figure 2(a), the regular ad-hoc node either generates a short distribution with most of the values equal to 0 when the node is not in the neighborhood, and equals to b_{max} when the node is located in the same neighborhood. In figure 2(b), the abnormal intermittent node (as seen by the other nodes) is characterized by a larger distribution of $X(v_i, v_j)$ values.



(a) Regular intermittent node

(b) Abnormal intermittent node

Fig. 2. Illustrative examples of the number $X(v_i, v_j)$ of hello packets periodically received by an ad-hoc node

Formal model of abnormal intermittence The main issue that we address is stated in two simple questions. Can we detect abnormal intermittence by monitoring simple parameters like for instance route state related ones? Can we do it in a distributed way such that malicious or non-cooperative nodes are outweighted? The perception of an abnormal intermittent node by an observing node can be modeled as a discrete Markov chain with four states: these four states depend on the functional state of the observed node (node up or node down), but also on the location of this node compared to the observing node (1-hop neighbor or not). From the perspectives of the abnormal intermittent node itself, the node behavior can be reduced to a discrete Markov chain with two states {NODE UP, NODE DOWN} with the transition probabilities p-failure and q-recovery that a node goes down and respectively goes up after a failure. The stationarity equation can be resolved to get the unique stationary distribution of this irreductible and positive recurrent Markov chain, as presented in equation 1 where p_{up} is the probability to be in state NODE UP and p_{down} is respectively the probability to be in state NODE DOWN.

$$(p_{up}, p_{down}) = (\frac{q}{p+q}, \frac{p}{p+q}) \tag{1}$$

In order to evaluate the impact of node abnormal intermittence (parameters p and q) on $X(v_i, v_j)$ distribution, we consider a simple scenario where v_i and v_j are in the same neighborhood, with v_i the observing node and v_j the observed abnormal intermittent node. During the measure interval $[t_l, t_{l+1}]$ (presented in figure 3), the probability of v_j to emit an hello packet at each r hello emission interval is given by p_{up}, the probability that the OLSR node v_j is up. Therefore, the probability for v_i of receiving k hello packets (and then the probability of not receiving $(b_{max} - k)$ hello packets) during $[t_l, t_{l+1}]$ follows a binomial distribution presented in equation 2.

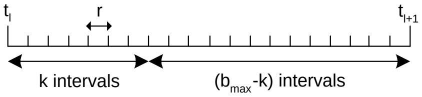


Fig. 3. Measure interval $[t_l, t_{l+1}]$ divided in b_{max} hello emission intervals

$$P(X_{v_i,v_j} = k) = \sum_{k=0}^{b_{max}} \begin{pmatrix} k \\ b_{max} \end{pmatrix} p_{up}^{k} (1 - p_{up})^{b_{max}-k} \tag{2}$$

This probability distribution will be considered to determine the impact of transition probabilities p and q on the observed fault behavior.

2.3 Beaconing Entropy Measure

We can monitor the OLSR routing protocol by performing an entropy measure of the probability distribution of $X(v_i, v_j)$. The entropy, defined by Shannon in [5], provides a measure of disorder for a system, where higher values indicate more disordered systems. In our case, it characterizes the distribution disorder (largest distribution) of hello packets for a neighbor node. Equation 3 defines the entropy measure noted $H(X(v_i, v_j))$ in a formal manner.

$$H(X_{v_i,v_j}) = \sum_{k=0}^{b_{max}} P(X_{v_i,v_j} = k).log(\frac{1}{P(X_{v_i,v_j} = k)}) \tag{3}$$

Let us consider the entropy measure for the examples presented in figures 2(a) and 2(b). $H(X_{v_i,v_j})$ equals 1.307 for a regular intermittent node, while $H(X_{v_i,v_j})$ reaches 2.642 for an abnormal intermittent node. High values of $H(X_{v_i,v_j})$ identify a disordered distribution with values $X(v_i, v_j)$ largely covering the interval $[0, b_{max}]$, and thus identify nodes with abnormal intermittence.

Assuming the discrete distribution of $X(v_i, v_j)$ given in equation 2, the entropy $H(X_{v_i,v_j})$ of this binomial distribution can be asymptotically approximated via analytic depoissonization as proposed by Jacquet and Szpankowski in [6] (see equation 4 where a_k are explicitly computable constants).

$$\begin{aligned} H(X_{v_i,v_j}) &\asymp \frac{1}{2} ln(b_{max}) + ln\sqrt{2\pi p_{up}(1-p_{up})} \qquad (4)\\ &\quad + \sum_{k\geq 1} a_k b_{max}^{-k} \\ &\asymp ln\sqrt{\frac{2\pi pq}{(p+q)^2}} + c \qquad (5) \end{aligned}$$

In equation 5, the approximated entropy $H(X_{v_i,v_j})$ is then given in function of the Markov chain's transition probabilities (p, q) (from equation 1) with the constant value $c = \frac{1}{2} ln(b_{max}) + \sum_{k\geq 1} a_k b_{max}^{-k}$. The impact of parameters $(p, q) \in]0, 1[^2$ can be estimated by studying the partial derivatives of $H(X_{v_i,v_j})$. This probabilistic entropy approximation provides an estimate of the additional entropy generated by an abnormal intermittent node (additional to the one generated by the mobility model), perceived from the point of view of a local node. It shows how abnormal intermittent nodes can be detected by a local node, by selecting the network nodes with the highest entropy $H(X_{v_i,v_j})$ of hello packets distribution. The reliability of this local measure can be improved by ad-hoc nodes collaboration.

2.4 Distributed Monitoring Approach

We presented in the previous section how the entropy measure of beaconing packets can locally detect abnormal intermittent nodes. The intermittence detection can be improved by sharing the local measurements among network nodes in a distributed manner. As depicted in figure 4, each ad-hoc node v_1, v_2, v_4, v_5, v_6 monitors locally the network nodes and exchange their local measurements to detect the abnormal intermittent node v_8. We will detail several distributed methods to synthesize the local measurements and to provide a more efficient and reliable intermittence monitoring at the network scale.

A detection approach consists in (1) ranking the potential abnormal intermittent nodes in the ad-hoc network according to a criteria c and then (2) selecting abnormal intermittent nodes according to a threshold value λ (nodes selecting are those presenting a criteria value $c(v_j) > \lambda$). We propose three detection methods and describe them below:

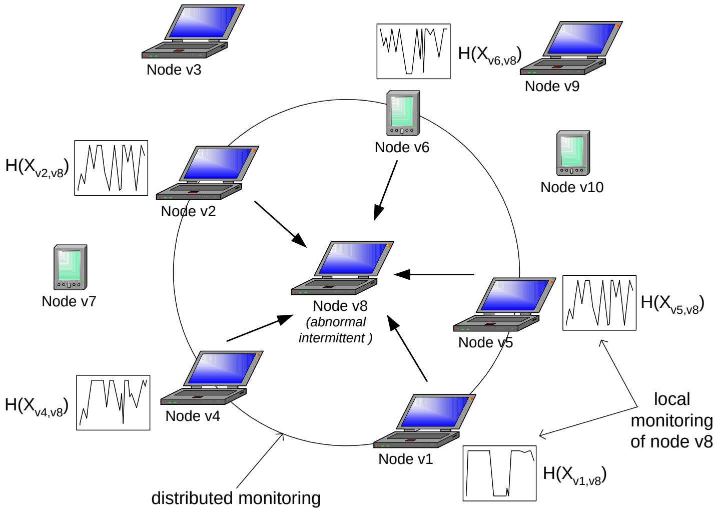


Fig. 4. Distributed intermittence monitoring

- The first detection method m_1 (called majority voting) defines a ranking of potential abnormal intermittent nodes in function of the number of observing nodes (which perceived the node as abnormal intermittent) in the network.
- The second method m_2 (called entropy sum) takes into account the number of observing nodes, but also the entropy values measured by these nodes. Therefore, m_2 ranks potential abnormal intermittent nodes in function of the sum of entropy values in the network. This method is actually an adaptation of method m_1 where results are weighted by entropy values.
- The last method m_3 (called entropy average) ranks potential abnormal intermittent nodes based on the average of measured entropy values. m_3 does not focus on the number of observing nodes, but favors the entropy values at the network scale.

These methods can be extended by weighting the measurements obtained from network nodes according to their reliability. Measurements from reliable nodes will have higher weights and then will be more taken into account in the detection process. The temporal coherence and the life time of monitoring data can be improved using approaches such as proposed in [7]. Their performance will be evaluated by simulation in Section 3.

3 Experimental Results

This section describes a set of simulations performed to evaluate the performance of the entropy-based monitoring with the different proposed detection methods, and to estimate the impact of the mobility model on this approach.

The experiments were performed with the discrete event network simulator ns-2 [8]. We simulated a mobile ad-hoc network of 50 nodes moving in a 1500 m x 300 m rectangular area during a time period of 900 simulated seconds. To avoid initialization discrepancy issues with the mobility model [9], we used the steady-state mobility model generator *mobgen-ss* where initial speeds and locations of nodes are chosen from the stationary distribution to perform an immediate convergence and provide more reliable simulations. For each experiment, a set of abnormal intermittent nodes is randomly chosen and follows the two-state Markov chain model with transition probabilities (p, q). This set of abnormal intermittent nodes is then compared to the set of nodes detected as abnormal intermittent nodes by the detection scheme.

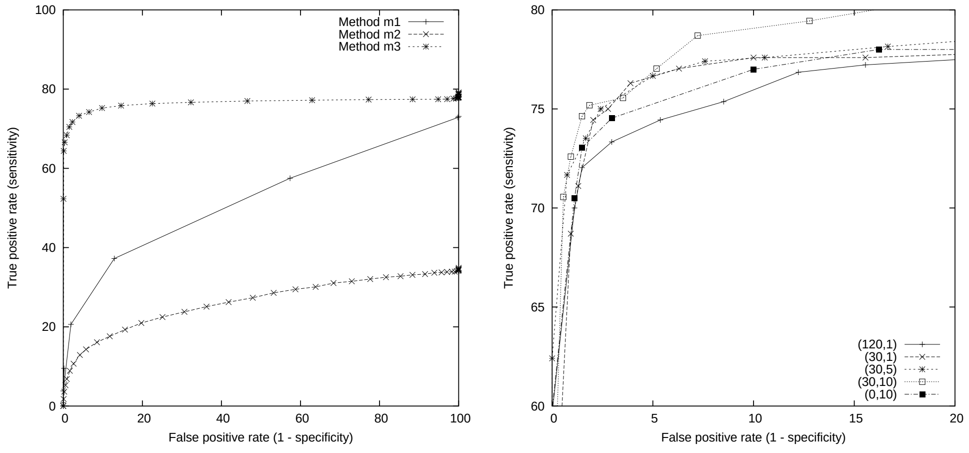
Table 1. Simulation parameters

Parameter	Value
Simulator	ns-2
Simulation time	900 s
Simulation area	1500 m x 300 m
Number of ad-hoc nodes	50 nodes
Number of abnormal nodes	0 - 5 node(s)
Mobility model	random waypoint *mobgen - steady state*
Speed	0.1 - 10 m/s
Pause time	0 - 120 s
Physical Layer	FSP / 2-RGR
MAC layer	IEEE 802.11
Routing layer	NRL OLSR

In order to quantify the performance of the approach, we performed an analysis of sensitivity and specificity. Our approach can be seen as a diagnostic test, where we test if an ad-hoc node is abnormal intermittent (positive test) or regular intermittent (negative test). The sensitivity shows how well the method picks up true cases (true positive or true negative results), while the specificity defines how well it detects false cases (false positive or false negative results). We use the receiver operating characteristic (ROC) [10], a graphical plot of sensitivity (Sn) versus 1-specificity (1 - Sp), to evaluate the detection efficiency. The ideal diagnostic method shows a plot that is a point in the upper left corner of the ROC space, as sensitivity (all true positives are found) and specificity (no false positives are found) reach both 1.0. A diagnostic method becomes random (and then inefficient) when it presents a line at an 45 degree angle from bottom left to top right, because the number of true positives equals the number of false positives. In the next parts of this section, we will detail the experimental results (1) by plotting and analyzing the ROC curves to compare the performance of the three detection methods and (2) by evaluating the impact of mobility model (random waypoint model with parameters $(pause, speed)$).

3.1 Performance of the collaborative detection methods

In a first set of experiments, we analyzed the performance of the three collaborative detection methods. These results are shown in figure 5(a) and are based on an extensive set of simulations with different mobility parameters $(pause, speed)$ and abnormal intermittence parameters (p, q). We varied node mobility with pause time *pause* from 0 to 120 s and with speed *speed* from 0.1 to 10 m/s. The abnormal intermittent nodes were parameterized with realistic transition probabilities. The failure probability p was set with low values from 0.1 to 0.2 and the recovery probability q from 0.1 to 1.0. For each individual setting we performed 150 simulations to assure the non-bias of the result.



(a) Comparison of methods m_1, m_2, m_3

(b) Impact of mobility on method m_3

Fig. 5. Evaluation of the collaborative detection methods with ROC curves.

The performance of the detection methods is summarized on figure 5(a), where we plotted the ROC curve for each method. A point (x,y) on a curve stands for the true positive rate (y) of the method compared to the false positive rate (x) for a given threshold value. We are interested in an optimal diagnostic method providing a low false positive rate for a maximum true positive rate. The closer a method is localized in the upper left corner of the ROC space, the more it provides an efficient detection. We can therefore deduct that method m_3 based on the average of entropies presents a better diagnostic test than the two others. In particular, method m_3 offers good results with a true positive rate of more than 70% in most of cases. In a more refined way, if we expect a false positive rate of less than 20%, method m_3 with 70% of true positive is definitively better than method m_1 providing a true positive rate of less than

45%, and still better than method m_2 showing a true positive rate of less than 20%. It turns out that methods m_1 and m_2 present less convincing performance, which can come from the simple fact that the detection is too dependent on the number of nodes observing an intermittent node. For instance for method m_1, the detection is based on the majority voting and consequently the probability of an ad-hoc node to be detected grows with the neighbor number of that node. In the same way, method m_2 considers the entropy sum at the network scale, which also raises in function of the number of neighbor nodes. In method m_3, using the average of entropies provides a more independent and reliable measurement of intermittence, where the increasing of the number of neighbors improves and refines the averaged measurement without denaturing it.

3.2 Impact of mobility model on intermittence detection

A natural question is whether mobility impacts the performance of the abnormal intermittence detection. Intuitively, higher mobility should make things worse: the entropy generated by mobility should hide the entropy generated by abnormal intermittence, but a precise quantification of this effect is required. A second series of experiments addressed this issue, where different mobility parameters were evaluated with a realistic intermittence (parameters $p = 0.1$ and $q = 0.4$). We varied the random waypoint parameters with reasonable pause time from 0 to 120 s and speed from 1 to 10 m/s, and measured the sensibility and specificity of the entropy average method m_3. These results are presented in figure 5(b) where we plotted the ROC curves for each couple $(pause, speed)$ of mobility parameters. We were interested in studying the detection method for configurations with low false positive rate and we therefore limited the plotting of ROC curves to a false positive rate no more than 20%. The comparison of ROC curves shows that the impact of mobility is relatively limited for realistic mobility scenarios. The variation between the lowest and the highest mobility parameters is indeed less than 5%. This statement comes from the nature of our measure, which actually highlights more the additional entropy generated by abnormal intermittence than the entropy generated by the network mobility. We expected that higher mobility implies bad results (i.e.: high speeds and short pause times), where by a low result we understand a low true positive rate for a false positive rate of less than 20 %. Such was the case indeed (note the case of $pause = 0$ and $speed = 50$) where the sensibility is less than 72%. A rather surprising result is however the case of lower mobility parameters where the sensibility is improved when mobility grows. This contradicts our initial hypothesis that mobility deteriorates our detection and leads us to more contrasted conclusion. The sensibility actually evolves in two steps. First, the detection is improved by mobility rise, from mobility parameters $(120, 1)$ to $(30, 10)$. The mobility increases the number of observing nodes per observed node. Second, the detection is noised with highest mobility scenarios and is not capable anymore to highlight efficiently abnormal intermittent nodes. In brief, the detection shows best results when mobility scenarios are not extreme (lowest and highest mobility parameters).

4 Related Work

Among the pioneering approaches in our context of fault management (we do not focus on intrusion detection/security), Jakobson introduces in [11] an approach for correlating events and faults with temporal constraints. Failures detection algorithms based on keep-alive messages (active approach) are experimented in [12] and their performance are evaluated in overlay networks. The OLSR hello mechanism corresponds to one of the experimented keep-alive approaches called gossip approach where a node periodically sends ”I'm alive” messages to its neighbors. Related work in monitoring the routing plane for fixed networks is described in [13], where a real-time system tracks the routing state of a single OSPF domain, using flexibly OSPF snooping and link state SNMP tracking. This system offers network statistics based on the monitoring of a link-state routing protocol, but it is mainly designed for performance analysis rather than fault detection. The DAMON architecture [14] defines a distributed monitoring system based on agents for multi-hop networks: agents perform the network monitoring and send to data repositories the measurements data. DAMON supports multiple data repositories and includes an auto-discovery mechanism of data repositories by the agents. This generic architecture is not dedicated to specific network parameters and could therefore be appropriate for the storage of fault monitoring data. WANMon is a monitoring tool described in [15] to monitor the resource usage in terms of network traffic, energy, memory and CPU, but its scope is limited to the host-level monitoring. Finally, our previous work in [16, 17] addresses an information model and a probe-based architecture for monitoring ad-hoc node participation.

5 Conclusions

We proposed in this paper a lightweight and distributed fault monitoring approach for ad-hoc networks and addressed the issue of detecting abnormal intermittence of ad-hoc nodes. The proposed solution is based on two key concepts: (1) a measure based on information theory to monitor intermittence over the routing layer and (2) a distributed scheme to perform abnormal intermittence detection among the network nodes. We have shown how correlating monitored data from different ad-hoc hosts provides an efficient and reliable detection of abnormal intermittence. We have proposed and evaluated different distributed methods based on fault ranking and thresholding methods. The main advantages of our approach are multiple: we can detect abnormal intermittent nodes even if they are not instrumented. The monitoring process is passive and completely decoupled from the OLSR protocol, without requiring any additional routing protocol piggybacking. Our future work will consist in assessing the intermittence monitoring with respect to different mobility models, defining an autoconfiguration mechanism for the collaborative detection methods and integrating the monitoring scheme into a management architecture.

References

1. Basagni, S., Conti, M., Giordano, S., Stojmenovic, I., eds.: Mobile Ad Hoc Networking. IEEE Press and John Wiley & Sons, Inc., Piscataway, NJ and New York, NY (2004)
2. Cover, T., Thomas, J.: Elements of Information Theory. Wiley & Sons (1991)
3. Kherani, A., Altman, E., Michiardi, P., Molva, R.: Non-cooperative Forwarding in Ad-hoc Networks. In: Proc. of the International IFIP Networking Conference (Networking'05), Waterloo, Canada (2005)
4. Clausen, T., Jacquet, P.: Optimized Link State Routing Protocol (OLSR). http://www.ietf.org/rfc/rfc3626.txt (2003) IETF RFC 3626.
5. Shannon, C.E.: A Mathematical Theory of Communication. The Bell System Technical Journal **27** (1948) 379–423
6. Jacquet, P., Szpankowski, W.: Entropy Calculation via Analytic Depoissonization. IEEE Transaction on Information Theory **45** (1999) 1072–1081
7. Westphal, C.: On Maximizing the Lifetime of Distributed Information in Ad-Hoc Networks with Individual Constraints. In: Proc. of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC'05), Urbana-Champaign, IL, USA (2005)
8. SAMAN: NS-2 Network Simulator. http://www.isi.edu/nsnam/ns/ (1989)
9. Yoon, J., Liu, M., Noble, B.: Random Waypoint Considered Harmful. In: Proc. of IEEE International Conference on Computer Communications (INFOCOM'03), San Francisco, CA, USA (2003) 1312–1321
10. Zweig, M., Campbell, G.: Receiver-Operating Characteristic (ROC) Plots: a Fundamental Evaluation Tool. Clinical Chemistry **29**(4) (1993) 561–577
11. Jakobson, G., Weissman, M.D.: Real-time Telecommunication Network Management: Extending Event Correlation with Temporal Constraints. In: Proc. of the 4th IFIP/IEEE International Symposium on Integrated Network Management (IM'95), Santa Barbara, CA, USA (1995)
12. Zhuang, S.Q., Geels, D., Stoica, I., Katz, R.H.: On Failure Detection Algorithms in Overlay Networks. In: Proc. of IEEE International Conference on Computer Communications (INFOCOM'05), Miami, FL, USA (2005)
13. Baccelli, E., Rajan, R.: Real-Time OSPF Route Monitoring. In: Proc. of the 7th IFIP/IEEE International Symposium on Integrated Network Management (IM'01), Seattle, WA, USA (2001)
14. Ramachandran, K., Belding-Royer, E., Almeroth, K.: DAMON: A Distributed Architecture for Monitoring Multi-hop Mobile Networks. In: Proc. of IEEE International Conference on Sensor and Ad Hoc Communications and Networks (SECON'04), Santa Clara, CA, USA (2004)
15. Ngo, D., Wu, J.: WANMON: a Resource Usage Monitoring Tool for Ad-hoc Wireless Networks. In: Proc. of the 28th Annual IEEE Conference on Local Computer Networks (LCN'03), Bonn, Germany (2003) 738–745
16. Badonnel, R., State, R., Festor, O.: Management of Mobile Ad-Hoc Networks : Evaluating the Network Behavior. In: Proc. of the 9th IFIP/IEEE International Symposium on Integrated Network Management (IM'05), Nice, France (2005) 17–30
17. Badonnel, R., State, R., Festor, O.: Management of Mobile Ad-Hoc Networks: Information Model and Probe-based Architecture. ACM International Journal of Network Management (ACM IJNM) **15**(5) (2005)