The Reliability of Detection in Wireless Sensor Networks: Modeling and Analyzing

Ming-Tsung Hsu[1], Frank Yeong-Sung Lin[1], Yue-Shan Chang[2], and Tong-Ying Juang[2]

[1] Dept. of Information Management, NTU,
No. 1, Sec. 4, Roosevelt Road, Taipei, 10617 Taiwan,
{d94004,yslin}@im.ntu.edu.tw
[2] Dept. of Computer Science and Information Engineering, NTPU,
No. 151, University Rd., San Shia, Taipei, 237 Taiwan,
{ysc,juang}@mail.ntpu.edu.tw

Abstract. A Wireless Sensor Network (WSN) composed of tiny sensor nodes may operate in an unfavorable terrain. The coupling of inherent limitations and harsh environments makes WSNs fallible. For this reason, reliability becomes one of the most important issues in WSN research. Some of the early work in the field of detection reliability focuses on collaborative effort. Instead of the collaborative work, the sensing improvements are proposed for detection reliability enhancement. Two types of detection models are constructed based on the scenarios of WSN operations for probability decomposition. The fault probability of detection and the probability of detection reliability in WSNs can then be estimated based on the decomposition of probabilities and empirical data. In analyzing the decomposition of probabilities, sensing improvements are shown to enhance detection reliability. An illustrative example is demonstrated to show how detection reliability can be controlled by different sensing improvements in different application situations.

Key words: Wireless sensor networks, Detection models, Detection reliability, Fault probability of detection, Sensing improvements.

1 Introduction

Recently, WSNs are developed and used for information collection [1], [7]. Including environmental monitoring, automatic controlling, and target tracking, WSN applications all have a data collection task. A tiny sensor node equipped with multifunctional sensors, a micro-processor, and a radio transceiver is responsible for this task.

The reliability becomes one of the most important issues in WSN research since sensor nodes are usually deployed in unattended and unfavorable environments, which makes each component of sensor nodes fault or crash easily. The techniques and mechanisms for the operations of sensing, processing, and communication are necessarily aware of this essential fact to maximize the reliability of WSNs. In this paper, sensing (detection) reliability is discussed in detail.

Faults in the sensing system, which is responsible for sensing environmental energies, may be caused by the hardware or software failure; may be produced by environmental noise; may last for a short or long time period; and can make the behavior of sensor nodes inactive or arbitrary. The results of sensing faults, such as the missing detection, false alarm, and unusual reading, can affect the data collection task severely, so they must be effectively overcome.

In most WSN applications, sensor nodes only send detection decisions or reports to a sink or a fusion center for energy conservation. For detection reliability improvement, the collaborative effort of a large number of sensor nodes is proposed previously [1], [6], [11], [13], [20]. Instead of the collaborative work, detection reliability is estimated by the analysis of detection models and enhanced by proposed sensing improvements in this paper.

In a detection-based (event-driven) WSN, there are four possible scenarios of a sensor node: (i) the sensor node misses an interesting event; (ii) the sensor node issues a false alarm; (iii) the sensor node accurately reports an interesting event; and (iv) the sensor node faultily reports an interesting event [11]. These scenarios show that the interesting event and detection error result in detection and there are four types of events (missing detection, false alarm, validity detection, and hidden fault detection) in the detection process.

The sensing system can be enhanced in different ways to increase detection reliability, e.g., increasing sensing capability may reduce the missing detection while increasing error resistance capability can avoid the false alarm. In this paper, four types of sensing improvements (including sensibility, dependability, effectiveness, and resistiveness) are theoretically defined.

The remainder of this paper is organized as follows: The detection models are constructed in Section 2. The fault probability of detection and the probability of detection reliability are also estimated in this section for detection models. Section 3 defines the sensing improvements and shows how to improve detection reliability theoretically. An illustrative example is depicted in Section 4 to demonstrate the effect of sensing improvements. Section 5 briefly reviews the related work of reliability in WSNs. Section 6 draws our conclusions and future work.

2 Detection Models

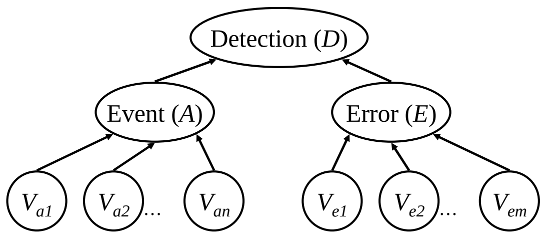
In this section, we first construct two types of detection models by the scenarios of WSN operations as mentioned previously. The fault probability of detection ($P(F_D)$) and the probability of detection reliability ($P(R)$) are also defined by the scenarios of WSN operations. $P(F_D)$ and $P(R)$ can be estimated based on the decomposition of probabilities or the observation of missing detection (M), false alarm (F), and hidden fault detection (H) in different detection models.

2.1 Model Construction

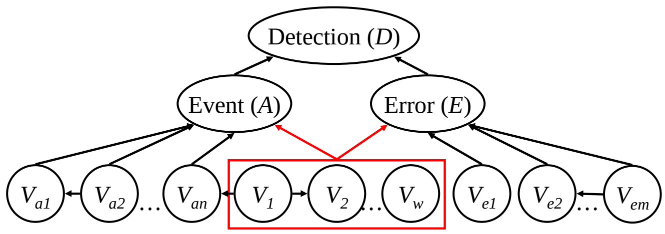
As introduced in Section 1, the interesting event (A) and detection error (E) lead to detection (D). Since A results from the environmental factors whose energies are sensed by sensor nodes and E also results from the environmental factors which make sensor nodes dysfunctional, A and E are thus both caused by environmental factors.

In an Independent Detection Model (IDM), A and E are affected by different environmental factors and these factors are mutually independent. Fig. 1(a) shows the structure of IDM. The intrusion detection system is an example of IDM, where infrared sensors sense the heat of objects (the environmental factor of intrusion events) and can be affected by high temperature and moisture (the environmental factors of errors) [1], [2].

The Conditionally Independent Detection Model (CIDM) is that A and E can be both affected by common environmental factors and/or the environmental factors affecting A and E are not mutually independent. Fig. 1(b) shows the structure of CIDM, where A and E are both affected by common environmental factors $(V_1, V_2, \ldots, V_w)$ and the environmental factors affecting A and E are not mutually independent. The forest fire tracking system is an example of CIDM where a fire event is detected and tracked as the temperature and humidity (the environmental factors of fire events) sensed by thermometers and hygrometers are both high, and an error may also be produced as the high temperature seriously affecting thermometers and hygrometers [1], [8].



(a) IDM: A and E lead to D and are affected by different and mutually independent environmental factors. The $(V_{a1}, V_{a2}, \ldots, V_{an})$ and $(V_{e1}, V_{e2}, \ldots, V_{em})$ are the environmental factors affecting A and E, respectively.



(b)CIDM: A and E lead to D and are both affected by common environmental factors and/or the environmental factors affecting A and E are not mutually independent.

Fig. 1. Detection models

2.2 Fault Probability of Detection

As introduced in Section 1, the operation of detection-based WSNs exists four possible events where M and F are widely discussed in the Signal Detection Theory (SDT). The fault probability of detection in SDT is defined as follows [20]:

Definition 1. *The fault probability of detection is defined by*

$$P(F_D) = P(A)P(\bar{D}|A) + P(\bar{A})P(D|\bar{A}) = P(A)P(M) + P(\bar{A})P(F) \ . \tag{1}$$

Based on Bayesian theorem and detection models, $P(M)$ can be decomposed as (2a) and (2b) for CIDM and IDM, respectively.

$$P(M) = \frac{P(\bar{D}|AE)P(AE) + P(\bar{D}|A\bar{E})P(A\bar{E})}{P(A)} \tag{2a}$$

$$P(M) = P(\bar{D}|AE)P(E) + P(\bar{D}|A\bar{E})P(\bar{E}) \ . \tag{2b}$$

In a similar manner, $P(F)$ of CIDM and IDM can also be decomposed based on Bayesian theorem as shown in (3a) and (3b), respectively.

$$P(F) = \frac{P(D|\bar{A}E)P(\bar{A}E) + P(D|\bar{A}\bar{E})P(\bar{A}\bar{E})}{P(\bar{A})} \tag{3a}$$

$$P(F) = P(D|\bar{A}E)P(E) + P(D|\bar{A}\bar{E})P(\bar{E}) \ . \tag{3b}$$

2.3 Probability of Detection Reliability

$P(F_D)$ is focused for detection reliability in most of previous work [6], [11], [13], [17], [20]. For example, in a WSN, $P(A)$ is 0.05 while $P(M)$ and $P(F)$ of senor nodes are 0.05 and 0.008, respectively. By Definition 1, $P(F_D)$ is 0.0101 and detection reliability might be treated as 0.9899.

It must be noted that errors are essential facts in WSNs and therefore, the correct detection $(D|A)$ can be differentiated into the validity detection and hidden fault detection. However, sensor nodes which faultily report interesting events should be considered as faulty. Considering that the hidden fault detection $(DE|A)$ may exist, the probability of reliability is defined as follows:

Definition 2. *The probability of detection reliability is defined by*

$$P(R) = 1 - (P(M) + P(H))P(A) - P(F)P(\bar{A}) \ . \tag{4}$$

The decomposition of $P(H)$ of CIDM and IDM by Bayesian theorem are shown in (5a) and (5b), respectively.

$$P(H) = \frac{P(D|AE)P(AE)}{P(A)} \tag{5a}$$

$$P(H) = P(D|AE)P(E) \ . \tag{5b}$$

2.4 Probability Estimation

To compute the probabilities in the subsection 2.2 and 2.3, $P(A)$, $P(E)$, and probabilities of D given A and E must be known.

$P(A)$ can be computed in (6a) and (6b) for CIDM and IDM, respectively, if all environmental factors affecting A are sensed. For the computing purpose, the value of environmental factors is assumed to be divided into levels.

$$P(A) = \sum_{i} \cdots \sum_{h} P(A|V_{a1,i} \cdots V_{w,h}) P(V_{a1,i} \cdots V_{w,h}) \tag{6a}$$

$$P(A) = \sum_{i} \cdots \sum_{l} P(A|V_{a1,i} \cdots V_{an,l}) P(V_{a1,i}) \cdots P(V_{an,l}) \tag{6b}$$

where $V_{an,i}$ and $V_{w,h}$ are the environmental factor V_{an} with level i and the environmental factor V_w with level h, respectively.

In a similar manner, $P(E)$ of CIDM and IDM can be computed by (7a) and (7b), respectively.

$$P(E) = \sum_{i} \cdots \sum_{h} P(E|V_{e1,i} \cdots V_{w,h}) P(V_{e1,i} \cdots V_{w,h}) \tag{7a}$$

$$P(E) = \sum_{i} \cdots \sum_{l} P(E|V_{e1,i} \cdots V_{em,l}) P(V_{e1,i}) \cdots P(V_{em,l}) \tag{7b}$$

where $V_{em,i}$ is the environmental factor V_{em} with level i.

In practical applications, $P(A)$ and $P(E)$ cannot be computed theoretically since some of environmental factors are difficult to sense. Instead of theoretically computing, the t-out-of-n rule [20] can be used to estimate $P(A)$ as sensor nodes are deployed densely. $P(M)$ and $P(F)$ of sensor nodes can also be estimated by counting the number of missing detection and false alarms [9]. $P(H)$ can be estimated as detection reports contain the energy readings of sensors. Since the error rate (including missing detection, false alarm, and unusual reading) of sensor nodes also can be computed by t-out-of-n rule, $P(E)$ can be estimated as the average error rate of all sensor nodes. $P(F_D)$ and $P(R)$ then can be estimated in practical applications as $P(A)$, $P(E)$, $P(M)$, $P(F)$, and $P(H)$ are known.

3 Theoretical Analysis

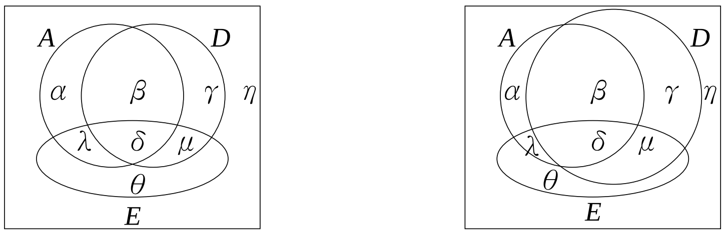
This section theoretically analyzes $P(M)$, $P(F)$, and $P(H)$ by proposed sensing improvements to minimize $P(F_D)$ and to maximize $P(R)$. For simplicity of analysis, Fig. 2, which illustrates the relationship among A, E, and D, is used in this section.

3.1 Sensing Improvements

The obvious method for improving $P(F_D)$ and $P(R)$ is that sensor nodes must be reinforced to resist the environmental interference and uncertainty. Based on the (2a), (2b), (3a), (3b), (5a), and (5b), the sensing improvements of sensor nodes can be classified as follows:

1. The sensibility improvement (S_S): the sensibility is the capability of a sensor node that it can report detection when only event occurs ($D|A\bar{E}$).
2. The dependability improvement (S_D): the dependability is the capability of a sensor node that it will not report detection when both error and event do not occur ($\bar{D}|\bar{A}\bar{E}$).
3. The effectiveness improvement (S_E): the effectiveness is the capability of a sensor node that it can report detection when both event and error occur ($D|AE$).
4. The resistiveness improvement (S_R): the resistiveness is the capability of a sensor node that it will not report detection when only error occurs ($\bar{D}|\bar{A}E$).

The capability of S_S, S_D, S_E, and S_R can be improved by decreasing the area of α, γ, λ, and μ or increasing the area of β, η, δ, and θ. In practical applications, these sensing improvements might be the trade-off and might not be improved simultaneously, e.g., improving S_S (increasing the area of D in Fig. 2(a)) might make S_R degraded (μ is increased and θ is decreased as in Fig. 2(b)).



(a) Relationship among A, E, and D. (b) Increasing S_S makes S_R degraded.

Fig. 2. Relationship among A, E, and D.

3.2 Probability Analysis

There are two parts in (2a) and (2b) for $P(M)$: one is the environmental interference ($\bar{D}|AE$) while another is the uncertainty ($\bar{D}|A\bar{E}$). Enhancing S_E can reduce the environmental interference and enhancing S_S can reduce the uncertainty.

Similarly, the reduction of $P(F)$ can be achieved when the S_R and S_D of sensor nodes can be enhanced to reduce the environmental interference ($D|\bar{A}E$) and the uncertainty ($D|\bar{A}\bar{E}$), respectively.

In IDM, $P(E)$ is the multiplier of sensing improvements in $P(M)$ and $P(F)$, which determines the efficiency of sensing improvements. As $P(E)$ is small, the effect of S_S is more than that of S_E for $P(M)$ and the effect of S_D is more than that of S_R for $P(F)$. Unlike IDM, the multiplier of sensing improvements in $P(M)$ and $P(F)$ for CIDM is the joint probabilities of A and E divided by the $P(A)$ or $P(\bar{A})$.

As shown in (1), $P(F_D)$ is the function of $P(M)$, $P(F)$, and $P(A)$, where $P(A)$ is the multiplier of $P(M)$ and $P(F)$. To reduce $P(F_D)$ needs to simultaneously reduce both of $P(M)$ and $P(F)$ in Bayesian detection problem [20]. Therefore, S_S, S_D, S_E, and S_R all affect $P(F_D)$ while $P(A)$ and $P(E)$ are the multiplier of sensing improvements in IDM and the joint probabilities of A and E are the multiplier of sensing improvements in CIDM.

$P(H)$ can be improved in (5a) and (5b) for CIDM and IDM, respectively, as S_E degraded. Then, $P(R)$ can only be affected by S_S, S_D, and S_R since S_E can reduce the environmetal interference in $P(M)$ but can also increase $P(H)$.

S_S, S_E, and S_R can be directly estimated from observation of empirical data, which is the same as discussed in subsection 2.4. S_D can be estimated by (3a) and (3b) for CIDM and IDM, respectively, as $P(F)$, $P(E)$, $P(A)$, the joint probabilities of A and E, and S_R are known.

4 Illustrative Example

Although Section 3 shows how to theoretically enhance $P(F_D)$ and $P(R)$, the impact of sensing improvements on $P(F_D)$ and $P(R)$ still needs to discern clearly. This section illustrates an example of IDM to show the impact of different sensing improvements in different application situations.

4.1 Intrusion Detection System

As mentioned in subsection 2.1, the intrusion detection system is an example of IDM. In an intrusion detection system, the prior probability used for probability computation can be obtained by empirical data or training data as discussed in subsection 2.4 and in [5], [9].

Based on the t-out-of-n rule, the probability of intrusion is observed by counting the times of intruder's arrival divided by the total time intervals in the empirical data, where at most one intrusion will occur in each interval.

$P(M)$ and $P(F)$ can be estimated by the average of missing detection and false alarm probabilities of each sensor node as shown in [9]. $P(H)$ can also be estimated by the observation as detection reports contain the energy readings. $P(E)$ can be estimated as the average error rate of all sensor nodes. The ratio of sensing improvements can be obtained as discussed in subsection 3.2. Table 1 lists these probabilities.

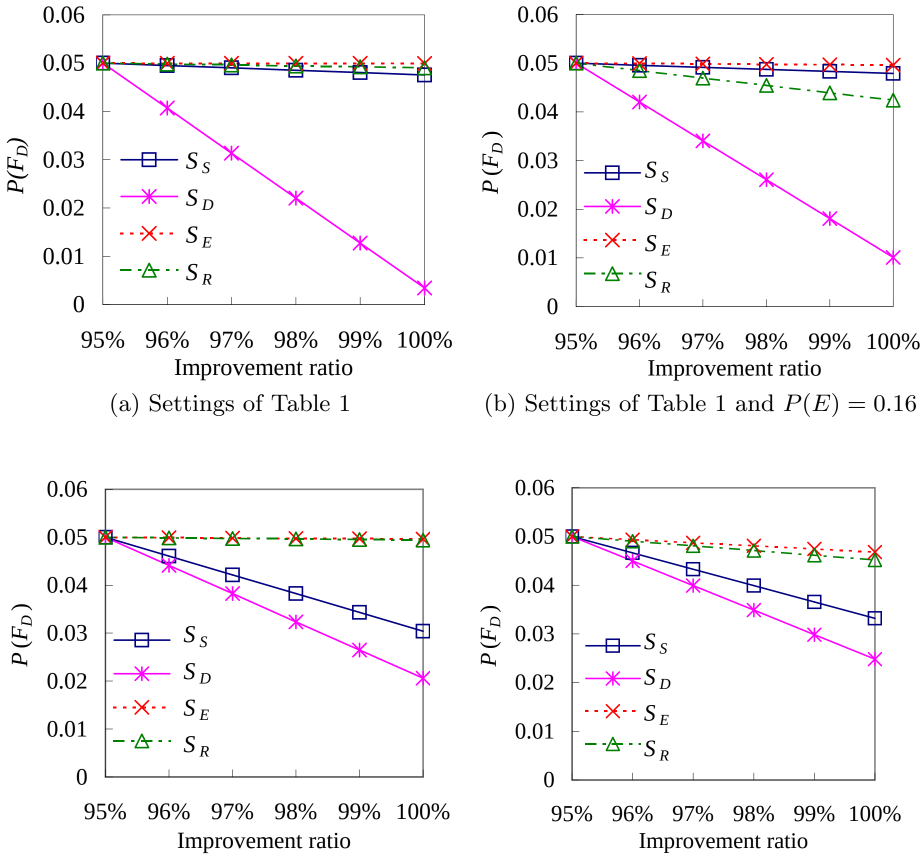
Table 1. The prior probabilities of an intrusion detection system

Event	True	False	Event	True	False	Event	True	False
A	0.050	0.950	E	0.020	0.980	M	0.050	0.950
F	0.050	0.950	H	0.019	0.981	$D\|A\bar{E}$	0.950	0.050
$D\|\bar{A}\bar{E}$	0.050	0.950	$D\|AE$	0.950	0.050	$D\|\bar{A}E$	0.050	0.950

4.2 Impact of Sensing Improvements

By the settings of Table 1, Fig. 3 shows the impact of different sensing improvements on $P(F_D)$. The slope of sensing improvements in figures means the decreasing speed of $P(F_D)$ and is determined by $P(A)$ and $P(E)$ as introduced in subsection 3.2.

In Fig. 3(a), S_S, S_E, and S_R scarcely affect $P(F_D)$, which reflects the small $P(A)$ and $P(E)$ of this example. Fig. 3(b) shows that S_R can reduce $P(F_D)$ as $P(E)$ increased. $P(E)$ can be treated as the weight of S_R for $P(F_D)$ in IDM. S_S can be used to reduce $P(F_D)$ as $P(A)$ increased, which is shown in Fig. 3(c). $P(A)$ can then be treated as the weight of S_S for $P(F_D)$ in IDM. In Fig. 3(d), S_D and S_S can reduce $P(F_D)$ efficiently in IDM as $P(A)$ and $P(E)$ are both increased. The effect of S_R is reduced as $P(A)$ increased in Fig. 3(c) and 3(d).



(a) Settings of Table 1

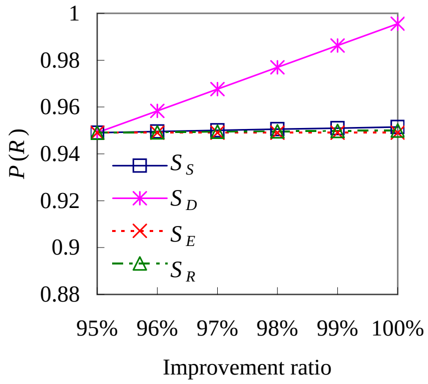
(b) Settings of Table 1 and $P(E) = 0.16$

(c) Settings of Table 1 and $P(A) = 0.4$

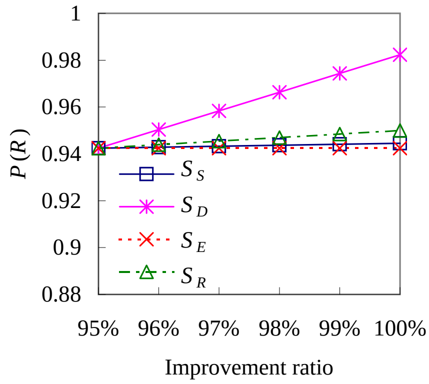
(d) Settings of Table 1, $P(E) = 0.16$, and $P(A) = 0.4$

Fig. 3. Impact of sensing improvements on $P(F_D)$

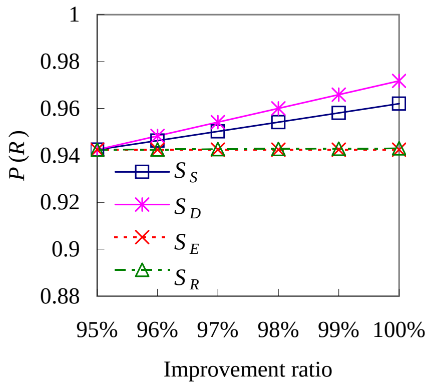
Fig. 4 shows that the effect of sensing improvements on $P(R)$ based on the settings of Table 1. The results of Fig. 4(a), 4(b), and 4(c) are the same as Fig. 3 while Fig. 4(d) shows that the $P(R)$ will be significantly affected by $P(H)$ as $P(A)$ and $P(E)$ are both large. In Fig. 3 and 4, S_E is shown to be less important in sensing improvements for $P(F_D)$ and $P(R)$ in IDM as $P(A)$ and $P(E)$ are small.



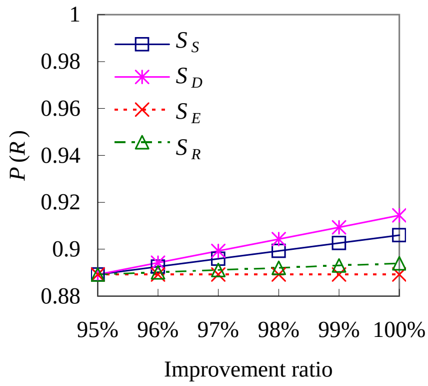
(a) Settings of Table 1



(b) Settings of Table 1 and $P(E) = 0.16$



(c) Settings of Table 1 and $P(A) = 0.4$



(d) Settings of Table 1, $P(E) = 0.16$, and $P(A) = 0.4$

Fig. 4. Impact of sensing improvements on $P(R)$

The results of the impact of sensing improvements on $P(F_D)$ and $P(R)$ shown in Fig. 3 and 4, respectively, are the same as that discussed in Section 3. In addition, they can provide the quantitative and illustrative information of sensing improvements.

5 Related Work

There are many approaches proposed to reinforce the reliability of WSNs. Most of these approaches are based on the collaborative work of sensor nodes since WSNs is generally deployed densely [1], [19].

For the purpose of reliable communication, Cerpa and Estrin [3] proposed an adaptive self-configuring routing protocol, named ASCENT, to establish a routing forwarding backbone by using a subset of sensor nodes; Chang, Hsu, Liu, and Juang [4] proposed a dependable geographical routing to dodge the faulty region; Ruiz, Siqueira, Oliveira, Wong, Nogueira, and Loureiro [14] used MANNA to identify the faulty sensor nodes and proposed a management scheme for event-driven sensor networks; and Staddon, Balfanz, and Durfee [15] proposed a tracing scheme in continuous sensor networks to monitor the crashed sensor nodes.

In reliable density control, Huang, Lo, Tseng, and Chen [10] proposed several decentralized protocols that schedule the duty cycle of sensor nodes to prolong the network lifetime while the sensing field is sufficiently covered; and Ye, Zhong, Cheng, Lu, and Zhang [18] proposed an adaptive scheduling approach, named PEAS, to ensure the coverage requirement of target area is fulfilled.

The fault tolerance mechanisms are also based on the collaboration of sensor nodes with the goal of reliable computing and detecting. Sun, Chen, Han, and Gerla [16] proposed a simple distributed technique, named CWV, by using neighbor's result and exploiting redundant information to discern local data dependability for improving reliability. Krishnamachari and Iyengar [11] proposed a scheme which let an individual sensor node use binary decisions of neighbors to correct its own decision to detect the event region for increasing fault tolerant capability. Luo, Dong, and Huang [13] enhanced this work by considering both measurement error and sensor node fault, which minimized the probability of detection error by choosing a proper neighborhood size in fault correction.

The collaboration of sensor nodes may cause the consistency problem when the Byzantine faults exist. Clouqueur, Saluja, and Ramanathan [6] proposed two fusion schemes, value fusion and decision fusion, to solve the Byzantine problem [12] and to accomplish better reliability in data fusion.

6 Conclusions and Future Work

Most WSNs are coupled with inherent limitations and harsh environments, which makes them fallible. The collected data might be flawed especially under the unfavorable conditions. The reinforcement of the reliability must be seriously considered before the deployment of WSNs and during the network operation.

In this paper, we show how to estimate $P(F_D)$ and $P(R)$ in different detection models. $P(R)$, which considers the hidden fault detection, is first proposed in the detection reliability research. We also discuss and analyze the impact of sensing improvements, including S_S, S_D, S_E, and S_R on $P(F_D)$ and $P(R)$. These sensing improvements can be obtained in laboratory experiments before sensor nodes are deployed and can be corrected in different applications by observed data as disscused in subsection 2.4 and 3.2.

The theoretical analysis illustrates the relationship among sensing improvements, $P(F_D)$, and $P(R)$. The enhancement in both of $P(F_D)$ and $P(R)$ are shown in Section 3. Further, the illustrative example of the intrusion detection system clearly shows how to control and improve $P(F_D)$ and $P(R)$ based on the different sensing improvements in different situations.

This paper shows that we can control detection reliability before the deployment of WSNs by default sensing improvements. $P(F_D)$ and $P(R)$ can then be used to compute the neighborhood size for collaborative work in the critical terrain as discussed in previous research. During the network operation, sensing improvements can be re-measured by practical data and the network protocols can be adapted by the information of $P(F_D)$ and $P(R)$.

The future work of this research will include the adaptive algorithm to rapidly adapt to the environmental interference for minimizing $P(F_D)$ and maximizing $P(R)$ during the network operation.

References

1. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Computer Networks **38** (2002) 393–422.
2. Biswas, P. K., Phoha, S.: Self-Organizing Sensor Networks for Integrated Target Surveillance. IEEE Trans. on Computers, **55(8)**, August 2006.
3. Cerpa, A., Estrin, D.: ASCENT: Adaptive Self-Configuring sEnsor Networks Topologies. IEEE Trans. on Mobile Computing, Special Issue on Mission-Oriented Sensor Networks, Volume 3, Number 3, July–September 2004.
4. Chang, Y.-S., Hsu, M.-T., Liu, H.-H., Juang,T.-Y.: Dependable Geographical Routing on Wireless Sensor Networks. Lecture Notes in Computer Science (LNCS) of Springer-Verlag, Vol. 4523, May 2007.
5. Chang, Y.-S., Juang, T.-Y., Lo, C.-J., Hsu, M.-T., Huang, J.-H.: Fault estimation and fault map construction in Cluster-based Wireless. The IEEE International Workshop on Ad Hoc and Ubiquitous Computing (AHUC 2006), Taichung, Taiwan, June 5–7, 2006.
6. Clouqueur, T., Saluja, K. K., Ramanathan, P.: Fault Tolerance in Collaborative Sensor Networks for Target Detection. IEEE Trans. on Computers, **53(3)**, pp. 320–333, March 2004.
7. Culler, D., Estrin, D., Srivastava, M.: Overview of Sensor Networks. IEEE Computer, Special Issue in Sensor Networks, Aug 2004.
8. Doolin, D. M., Sitar, N.: Wireless sensors for wildfire monitoring Proceedings of SPIE Symposium on Smart Structures & Materials/ NDE 2005, San Diego, California, March 6–10, 2005.
9. Hsu, M.-T., Lin, F. Y.-S., Chang, Y.-S., Juang, T.-Y.: The Fault Probability Estimation and Decision Reliability Improvement in WSNs. Proceedings of the IEEE Region 10 Annual International Conference (TENCON 2007), Taipei, Taiwan, Oct. 30–Nov. 2, 2007.
10. Huang, C.-F., Lo, L.-C., Tseng, Y.-C., Chen, W.-T.: Decentralized Energy-Conserving and Coverage-Preserving Protocols for Wireless Sensor Networks ACM Trans. on Sensor Networks, Vol. 2, No2, May 2006.

11. Krishnamachari, B., Iyengar, S.: Distributed Bayesian Algorithms for Fault-Tolerant Event Region Detection in Wireless Sensor Networks. IEEE Trans. on Computers, **53(3)**, pp. 241–250, March 2004.
12. Lamport, L., Shostak, R., Pease, M.: The Byzantine Generals Problem. ACM Trans. on Programming Languages and Systems, **4(3)**, pp. 382–401, July 1982.
13. Luo, X., Dong, M., Huang, Y.: On Distributed Fault-Tolerant Detection in Wireless Sensor Networks. IEEE Trans. on Computers, **55(1)**, Jan. 2006.
14. Ruiz, L., Siqueira, I., Oliveira, L., Wong, H., Nogueira, J., Loureiro, A.: Fault Management in Event-Driven Wireless Sensor Networks. ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, 2004 (MSWIM'04).
15. Staddon, J., Balfanz, D., Durfee, G.: Efficient Tracing of Failed Nodes in Sensor Networks. First ACM International Workshop on Wireless Sensor Networks and Applications, Sep 2002.
16. Sun, T., Chen, L.-J., Han, C.-C., Gerla, M.: Reliable Sensor Networks for Planet Exploration. The 2005 IEEE International Conference On Networking, Sensing and Control (ICNSC'05).
17. Varshney, P.: Distributed Detection and Data Fusion. Springer-Verlag, 1996.
18. Ye, F., Zhong, G., Cheng, J., Lu, S., Zhang, L.: PEAS: A Robust Energy Conserving Protocol for Long-lived Sensor Networks. Proceedings of the 23rd International Conference on Distributed Computing Systems (ICDCS'03).
19. Zhang, H., Hou, J. C.: Maintaining Sensing Coverage and Connectivity in Large Sensor Networks. Wireless Ad Hoc and Sensor Networks: An International Journal, Vol. 1, No. 1–2, pp. 89–123, January 2005.
20. Zhang, Q., Varshney, P.K., Wesel, R.D.: Optimal Bi-Level Quantization of i.i.d. Sensor Observations for Binary Hypothesis Testing. IEEE Trans. Information Theory, vol. 48, no. 7, pp. 2105–2111, 2002.