Immune-Inspired Self Healing in Wireless Sensor Networks

TiongHoo Lim[1,3], HuiKeng Lau[1,4], Jon Timmis[1,2], and Iain Bate[1]

[1] Department of Computer Science, University of York
[2] Department of Electronics, University of York,
Heslington, YO10 5DD, UK
[3] Electrical and Electronics Engineering,
Institut Teknologi Brunei, Tungku Link, Gadong BE 1410, Negara Brunei Darussalam
[4] School of Engineering and IT, Universiti Malaysia Sabah,
88999 Kota Kinabalu, Sabah, Malaysia
{tl540,hl542,jon.timmis,iain.bate}@york.ac.uk

Abstract. Link failure and unreachable nodes due to interference from external devices are common problems in WSNs. These interferences can be a major inhibitor to node performance and network stability. In order to tolerate these failures, we propose an immune-inspired self healing system where an individual node can detect degradations in network performance, perform diagnostic tests, and provide automated immediate response to recover the network to a stable state. We evaluate and compare the performance of our approach with other routing protocols on a testbed environment using TelosB hardware motes.

Keywords: wireless sensor networks, error detection, error classification, error recovery, receptor density algorithm, routing protocol.

1 Introduction

Advances in microchip and communication technologies have enabled mass production of small and cheap devices called sensor nodes that are capable of sensing the environment and interact with each other. These nodes interact over the radio channel to form wireless sensor networks (WSNs) [1]. Each node can operate autonomously to monitor and collect data, and send the data packet over the wireless network via multi-hop routing protocols. To date, it has been used for indoor and outdoor applications such as remote patient health monitoring, fire search and rescue operation, and disaster management [1]. This type of application requires a specific level of quality of service (QoS) and availability of real-time data from the nodes to allow informed decisions and actions to be made.

An important issue is, real-world implementations of WSNs are usually difficult to control and susceptible to anomalies [19]. Anomalies, such as communication failure caused by battery depletion, component malfunction, human activity, obstruction, and interference, may occur in WSNs. This is in particular true when other devices operating at the same radio frequency as WSNs, e.g.

C.A. Coello Coello et al. (Eds.): ICARIS 2012, LNCS 7597, pp. 42–56, 2012.

IEEE 802.11 devices, are deployed very close to the sensor nodes [18]. The interferences created by these devices may exhibit unique and distinct characteristics that can be classified into different categories. In order for WSNs to operate over extended periods of time, individual nodes must be able to tolerate these interferences effectively. This can be achieved with a combination of detection, diagnostic and recovery mechanisms.

Over the years, many immune-inspired anomaly detection systems (ADSs) have been successfully applied to WSNs. This is partly motivated by the analogy between the characteristics of WSNs and the immune system. The Dendritic Cell Algorithm [8] and Negative Selection Algorithm [5] have been successfully applied to detect network and traffic anomalies. To be able to establish the anomalies that can lead to major failures is essential. Drodza et al. [4] applied the interaction between innate and adaptive immunity to classify the errors that can lead to degradation in packet delivery rate. However, these works mainly focus on detection, not on recovery. If real time remedial action is not performed, the network condition is likely to get worse. Recently, an automated response system based on Cognitive Immune System (CIS) has been proposed in [17] to network failure that assumed an accurate detection system is present to trigger the response system. However, detection without effective diagnosis of network disruptions is not sufficient to determine the underlying cause of the problem, and confirm the presence of the interference for an appropriate remedial action to be taken. These three actions have to be integrated into one component. In addition, for all these studies, the proposed solutions mainly focused on failure caused by malicious attacks. These attacks usually have unique features that can easily be detected. Little work has investigated anomalies due to interference in the operating environment, either using ADSs or with more conventional approaches. One of challenges in detecting anomalies due to interference is that the duration and occurrence for these type of anomalies are unpredictable and changes with time [14]. Thus, it is difficult to be detected and classified using existing AIS or conventional approaches [2].

In this paper, we propose an integrated immune-inspired Interference Detection and Recovery System (IDRS) based on CIS [3] to allow individual nodes to detect, diagnose and make decision as to how to response to network failure due to radio interference. The CIS postulates that the immune systems do not only protect the body, but it also performs body maintenance through the process of recognition, cognition and response, with respect to its environment [3]. Based on this principle, we combine the use of the Multi-modal Routing Protocol (MRP) [11] and the Receptor Density Algorithm (RDA) [15]. The MRP is a multi-modal routing protocol proposed to overcome transmission failure by providing automated responses based on existing routing protocols. The RDA is an artificial immune system algorithm based on a T-Cell signalling model with statistical kernel density function to detect anomalies [15]. The main contributions of this paper are 1) A novel distributed anomalies detection, diagnostic, and recovery system that can identify and respond to network anomalies caused by radio interference, 2) The application of the RDA as a diagnostic tool to identify the

different types of interference in the radio channel and to aid recovery decision, and 3) A quantitative evaluation of the proposed IDRS.

The remaining of the paper is structured as follows. Section 2 formulates the problem before an insight into the design and implementation of the proposed IDRS design and algorithm is presented in Section 3. The accuracy, efficiency and reliability of IDRS are evaluated and discussed in Section 4. Section 5 ends the paper with the conclusion and future work.

2 Radio Interference in Wireless Sensor Network

Network failures in WSNs due to interference are common as WSNs uses the same radio frequency with other devices such as portable phones, microwave ovens, Bluetooth devices, and Wi-Fi networks. Lin et al. [13] has classified the radio interference in three distinct patterns namely: small fluctuation created by multi-path fading of wireless signals; large disturbance due to shadowing effect of the presence of obstacles; continuous large fluctuations caused by Wi-Fi devices. Each of these interference patterns can have different decremental effects on the Packet Sending Ratio (PSR). Recent work by Wang et al. [18] has shown that due to interference from a Wi-Fi network, packet loss in WSNs can reach up to 30%. To overcome this interference, the nodes may need to retransmit their packet, or even increase their transmission power in order to communicate with their neighbour. In other cases, when the interference source is strong, the node may need to establish a new route in order to send the packet. All these recovery steps may aggravate a congested network and reduce the availability and lifetime of the network if it is not executed according to the interference patterns.

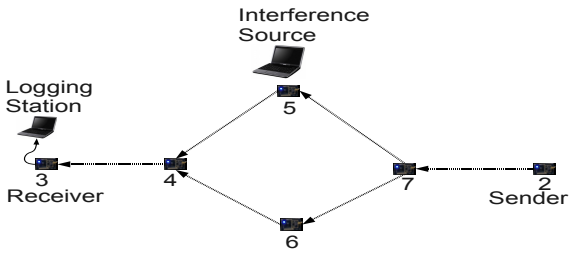

Fig. 1. Interference source is introduced near node 5 to disrupt the radio communication between node 2 and 3

To illustrate, six static and functionally homogeneous sensor nodes can be deployed in the topology shown in Fig.1. Each sensor node is capable of packet forwarding and produce network statistics. When a Wi-Fi device is placed close to node 5, the communication between node 5 and its neighbouring nodes (node 4 and 7) can be disrupted resulting in packet loss. As a result, the affected nodes will attempt to recover from the transmission failure by executing protocol-specific recovery functions such as retransmission, flooding and collision

avoidance [16]. However, these responses are only effective if they are applied correctly, depending on the durations and intensity of the interference. Hence, it is not only a matter of detecting the presence of an anomaly, but also the cause of an anomaly, in order to make accurate and automated recovery decision.

3 IDRS: Interference Detection and Recovery Systems

The immune-inspired Interference Detection and Recovery System (IDRS) serves two purposes:

1. to accurately identify the interference that is affecting the communication between a node and its neighbour in a distributed manner,
2. to make autonomous decision on the recovery action to mitigate the effect of the interference, and improve the network reliability and efficiency.

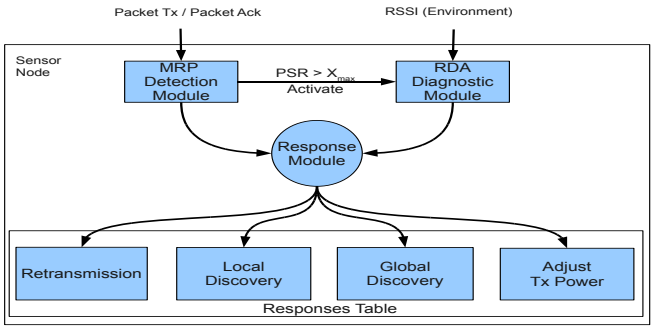

Fig. 2. The architecture of the CIS-based Interference Detection and Recovery System

The IDRS (Fig.2) consists of three modules, representing each stage in the CIS: MRP Detection Module (MDM), RDA Diagnostic Module (RDM), and Radio Interference Response Module (RIRM). Inputs to the IDRS are the PSR and the Receive Signal Strength Indicator (RSSI). These inputs can easily be obtained and calculated from the node. The MDM acts as the first line of defence to provide early detection and response to the interference when PSR is less than a predefined threshold value. If the condition does not improve, the MDM will activate the RDM to identify the type of interference based on the RSSI. Based on the results from both the MDM and the RDM, the RIRM will activate one or a combination of responses based the cognitive theory of *regeneracy* [3]. By using the close feedback loop provided by link layer, the effectiveness of the responses can be evaluated by the MRP. The cost of each response will be adjusted accordingly. Hence, IDRS is able to recognise and respond more effective from novel or existing interference based on the history of the response, and the strength and duration of the interference.

In the following subsections, a detailed description of the proposed IDRS Algorithm, in Appendix, is presented.

3.1 MDM: The MRP Detection Module

In WSNs, the packet reception ratio (PRR) is commonly used as a metric to detect network anomalies. The PRR is shared between neighbouring nodes [12]. This data is usually piggybacked on existing packet. However, in the presence of interference this data may be lost or corrupted. Hence, we advocate that the detection module should be implemented at the transmitting node. In the IDRS, we propose the use of the MRP [11] to detect the presence of interference based on the PSR and provide an initial response. The PSR is the total number of packets successfully send over the total number of attempts made in a given time window. The MRP detects deviation in the PSR and utilises the packet acknowledgement (P_{ack}) to provide network recovery responses [11] and to activate the RDM. Each route recovery response incurs a specific cost (RT_{cost} for *retransmission*, LD_{cost} for *local recovery*). Associated with each recovery response is a maximum cost threshold: RT_{max} for retransmission, and LD_{max} for recovery. The recovery response will only be selected if the cost of carrying out the response is lower than the maximum threshold. All these responses utilise the existing acknowledgement mechanisms on the link layer. As such, no additional communication overhead is incurred in the network. Work by Lim et al. [11] has demonstrated by employing MRP, significant network improvement has been achieved.

3.2 RDM: The RDA Diagnostic Module

To identify the cause of a transmission failure, the Received Signal Strength Indicator (RSSI) is used. Monitoring the RSSI in WSNs has been widely used to decide the required transmission power to transmit a packet [2,12]. However, as illustrated in Fig.3 (a_1) and Fig.3 (a_2), the RSSI values are sensitive to changes in environment. It has been demonstrated to be a challenging task to classify the RSSI values with traditional statistical techniques [2]. Small changes in the operating environment can trigger large variations in the RSSI, making it difficult to accurately determine the type of interference [9]. Here, we propose the use of the RDA [10,15] to filter the background noise and classify the interference. The RDA has been used to detect partial failure in swarm robotic system [10] and chemical substances [7] with high positive detection rate and low false detection rate. Its ability to recognise anomalies in a dynamic environment has motivated its application to WSNs.

The RDA was developed based on the immunological modelling on the activation of the T Cell Receptor (simply referred to as the *receptor* in this paper) when presented with antigen on the surface of an antigen presenting cell [15]. Depending on how often the receptor encounters the antigen, the receptor can become more sensitive or less sensitive (lower activation threshold) towards the antigen. To apply the RDA, the input data is divided into s discretised locations and a *receptor* $\mathbf{x}_s$ is placed at each of these locations. A receptor has a length $\ell = (\sqrt{2\pi})^{-1}$, a position $r_p \in [0, \ell]$, and a negative feedback $r_n \in (0, \ell)$. At each time step t, each receptor takes input $\mathbf{x}_i$ and performs a binary classification $c_t \in 0{,}1$ to determine whether that location is considered anomalous. The

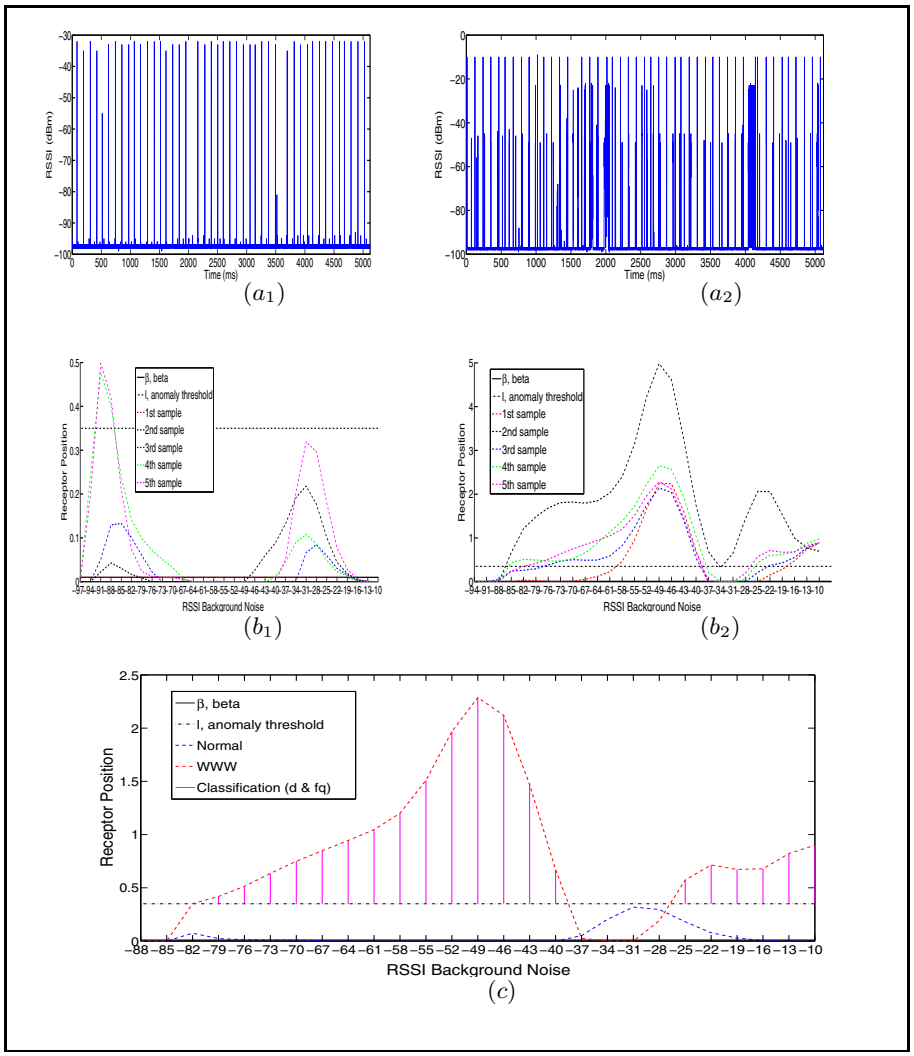

Fig. 3. The raw RSSI data collected (both normal (a_1) and abnormal (a_2) samples) from the radio interface are fed into RDA to product normal (b_1) and abnormal (b_2) signatures of activated receptors. Using the outputs generated by RDA, the interference can be classified into either Class I, II, or III based on the euclidean distance of the furthest activated receptor and the number of activated receptors above the threshold l, represented by the global maximum and vertical lines in (c) respectively

classification decision is determined by the dynamics of r_p and negative feedback $r_n \in (0, \ell)$.

The process for initialisation and classification of the RSSI values are described as follows:

Phase 1: Initialisation

1. Present the normal RSSI values $\mathbf{X}$ (Figure $3a_1$) to the RDA to generate its normal signature (Figure $3b_1$). For each receptor x , calculate the sum of stimulation $S(x)$ on each receptor x for each RSSI input x_i, $x_i \in \mathbf{X}$.

$$S(x) = \sum_{i=1}^{n} \frac{e^{\frac{-(x-x_i)^2}{2h^2}}}{h\sqrt{2\pi}} \tag{1}$$

   where h is the kernel width and set to 5 in this paper, and n is the total number of normal RSSI values.
2. Calculate the negative feedback $r_n(x)$ for each receptor x. The base negative barrier β is set to a small value, 0.01 in this paper.

$$r_n(x) = \begin{cases} S(x) - \beta, & \text{if } S(x) \geq \beta \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

Phase 2: Classification

1. Initialise the receptor position $r_t(x)$=0 for all receptors.
2. Based on the MAX($r_p(x)$) of normal signature, set the threshold value of the receptor length $\ell = (\sqrt{2\pi})^{-1}$.
3. Calculate the new receptor position $r_p(x)$ with current RSSI values $\mathbf{V}$.

$$K_s = \sum_{i=1}^{n} \frac{e^{\frac{-(x-v_i)^2}{2h^2}}}{h\sqrt{2\pi}}, \qquad r_p(x) = K_s - r_n(x) \tag{3}$$

   where each RSSI value $v_i \in \mathbf{V}$.
4. Classify $\mathbf{V}$:
   A receptor is activated when

$$\mathbf{V} = \begin{cases} Normal, & \text{if } r_p(x) < l \\ Interference, & \text{otherwise.} \end{cases} \tag{4}$$

   The classification of v to different classes of interference is based on two variables (Figure 3c):
   - The difference between distance of the highest receptor position and ℓ ($\max(\ell - r_p(x))$), referred to as *Intensity*;
   - The number of activated receptors, referred to as *Duration*.

3.3 RIRM: The Radio Interference Response Module

We assume that based on the RSSI and the PSR values, the interference can be classified into three classes according to the different duration (short or long) and intensity (weak or strong). Also, four different responses can be used to overcome the interference:

1. Retransmission (RT): Retransmission is the default action and activated when the MDM detects that the acknowledgement packet P_{ack} is not received and the cost of retransmission RT_{cost} has not exceed the threshold RT_{max}. This response is particularly effective when the interference noise signal is *weak* and *short* (CLASS I).
2. Local Discovery (LD): Local discovery is activated when the node failed to send the packet after several RT attempts (as indicated by PSR lower than 90%) or when the RDM identified a CLASS II interference. This response is best executed only when the next node is unavailable and the interference noise signal is *weak* and *long* (CLASS II).
3. Global Discovery (GD): This is usually the last option to take when the existing route is known to be unreliable. This action is usually taken when all the previous responses have failed, and there is no local node available to re-route the traffic, or the interference source is *strong* and *long* (CLASS III).
4. Transmission Power Control (TPC): This is an additional response to handle unavailable route cause by node failure or obstruction. It is a common approach to increase the transmission power in order to communicate with the next hop neighbouring node [2,12]. However, the use of higher transmission power can only be applied when necessary as it consumes more battery power and can interfere with other nodes. Hence, TPC is only applied when CLASS I interference is detected with the PSR is lower than 90% and the transmission power Tx_{power} is less than a predefine maximum power Tx_{max}.

To clarify, a decision tree, based on expert knowledge, is presented in Figure 4 to show the response strategy to be selected based on the current network environment.

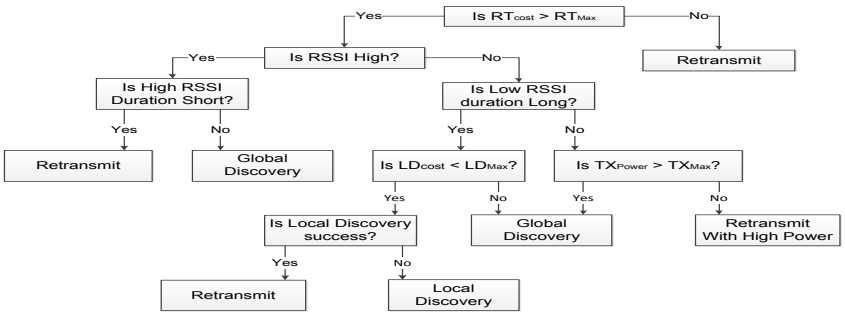

Fig. 4. Decision tree based on the RIRM and MDM to response to different interference

4 Experiments and Results

In order to evaluate the proposed IDRS, we conducted two experiments. The first experiment examines the effectiveness of the RDA classifier in the RDM whilst the second experiment evaluates the efficacy of the proposed IDRS when compared to other methods.

4.1 Evaluation of the RDM

In the RDM, we use over 850,000 RSSI readings to classify the interference into three classes: CLASS I, CLASS II, and CLASS III. The RSSI values are obtained from the TelosB radio module, exposed to different interference source. The spectrum of the RSSI values used is the range of -100dBm to -10dBm. This spectrum is uniformly divided into 30 slots and a receptor is used to represent each slot (the value x in Eq. 1).

In order to classify the interference into the three classes, an unsupervised K-mean clustering algorithm is applied to the set of training data (offline). The derived classes based on *Intensity* (**C1**) and *Duration* (**C2**) are in Table 1.

Table 1. Interference Class

Intensity, C1	**Duration, C2**	Class	Remarks
$0 <$ **C1** ≤ 2.8	$0 <$ **C2** ≤ 5	I	weak intensity, short duration
$2.8 <$ **C1** ≤ 11.0	$5 <$ **C2** ≤ 16	II	weak intensity, long duration
C1 > 11.0	**C2** > 16	III	strong intensity, long duration

We evaluate the performance of the RDM in TelosB mote based on *sensitivity* (Eq. 5) and *precision* (Eq. 6).

$$Sensitivity = \frac{TP}{TP + FN} \quad (5) \qquad Precision = \frac{TP}{TP + FP} \quad (6)$$

Sensitivity measures how well the RDM can correctly classify the interference source whilst *precision* measures the probability of a detected event is representing a true positive result rather than a false positive. *Precision* ensures the appropriate response is taken for the corresponding interference.

Experimental Setup: Two static nodes are deployed across a distance of 10 metres. One node is configured to transmit packets at the rate of 8 packets per second while sampling its radio channel at the rate of 1 KHz to collect the RSSI values and perform online detection.

Eight different network conditions are used to test the system namely: normal WSN communication, object blocking, jamming from another node, Wi-Fi traffics such as web browsing (WWW), slow video streaming, fast video streaming,

slow file downloading, and fast file downloading. In each run, only one type of interference was injected into the network at periodic interval. This is done by placing a laptop next to the receiving node. Due to the limited log size in the motes, each experiment was run for 5 minutes to generate 2400 packets and is repeated 15 times.

Experimental Results: The results for the experiment are shown in Table 2. In the table, the RDM achieved a precision above 80% for most of interferences especially for interferences that have drastic impact on the PSR (PSR $< 70\%$) such as blocking and fast download. These two types of interference require a different recovery approach. Hence, it is important to achieve a precision rate above 80% precision rate to allow a specific response approach to be taken when PSR $< 75\%$. Although the false negative rate for Class II interference is high due to misclassification, its impact on the network PSR is less extreme with only up to 25% packet loss compared to blocking and fast download with packet loss above 30%. Beside, high accuracy in Class II interference is usually not required for accurate response as the sequential recovery step provided by the RIRM will eventually trigger the right response.

Table 2. The sensitivity and precision of the RDM in classifying different sources of interference. The RDM showed high sensitivity and precision for Class I and III interference.

Interference Source	Class Type	True Positive	False Positive	True Negative	False Negative	Sensitivity	Precision	PSR (Ave)
Normal	I	98	0	0	0	100.00%	100.00%	95%
Blocking	I	47	0	3	0	100.00%	**100.00%**	68%
Jamming	I	30	5	28	0	100.00%	**85.71%**	70%
WWW	II	12	10	7	8	60.00%	54.55%	80%
Slow Streaming	II	54	0	23	49	52.43%	**100%**	81%
Slow Download	II	14	5	2	4	77.78%	**73.68%**	76%
Fast Streaming	III	14	1	23	4	77.78%	**93.33%**	63%
Fast Download	III	39	8	13	6	86.67%	**82.98%**	45%

4.2 Evaluation of the IDRS

In this experiment, the performance of the IDRS will be compared to the Not So Tiny's AODV (NST) [6], the original MRP [11], and a modified MRP with TPC (M_{TPC}). M_{TPC} protocol is used to evaluate the benefit of boosting the transmission power with or without RDM. The performance of the routing protocols is evaluated based on the following metrics:

– **Packet Delivery Ratio (PDR)**: PDR represent the percentage of the number of packets received by the receiver, to the total number of packets

transmitted by the sender. This metric measures the reliability of the routing protocol.

- **Transmission Overhead (TO)**: TO is defined as the average number of transmissions made by a node to deliver the packets to the receiver. This metric represents the efficiency of the routing. It can be calculated by dividing the sum of the transmissions made, including RT, LD and GD, to the total number of packets received.
- **Average Current Consumption (CC)**: CC can be determined by first calculating the total currents, $I_{total}(i)$ consumed in a node, i, by multiplying the number of packets transmitted to the current required to transmit one packet at that power level. A typical current consumption for transmitting a packet can be obtained from the Chipcon data sheet[1]. Finally, $I_{total}(i)$ can be used to determine the network average current consumption by multiplying $I_{total}(i)$ to the total of nodes in the networks.

Experimental Setup: Six static TelosB motes are placed 3 metres apart using the topology shown in Fig.1. The experiment is conducted at the centre of a room relatively free from uncontrolled radio sources to ensure its correctness and validity. The node transmission is set to minimum power using the same channel as the Wi-Fi in the room to treat it as a source of interference. The LLN is enabled to allow packet acknowledgement. During initialisation, node 2 is configured to collect temperature reading from the sensor and transmit the packet to node 3, at regular intervals of 256ms via the intermediate nodes. Once the network route has been established, and the normal signature has been collected by the RDM (after 30 seconds), different sources of interference are introduced into the network (close to node 5) at 30 seconds intervals. Each interference lasts for approximately 15 seconds. Each test is run for 10 minutes and is repeated 15 times.

Experimental Results: The results for this experiment are shown in Table 3. The results show that the IDRS outperformed the other three routing protocols in term of energy efficient (CC) when interference was introduced. Under the normal condition, all routing protocols consumed similar amount of energy to transmit one packet successfully. However, when interference was introduced, higher *TO* (up to an average of 14 transmissions per packet) has been observed in NST as NST requires to retransmit the packet before performing local discovery. The *TO* is significantly less for routing protocols with MRP especially for IDRS as highlighted in Table 3. As a result, less current is used to deliver a packet successfully.

When interferences with longer duration (CLASS II and CLASS III) are introduced, the IDRS consumed the least current as precise response can be executed by RIRM based on the diagnosis made by the RMD. For example, as shown in Table 4 with Class II interference, the IDRS performed less RT and TPC as the node was able to recognise the interference and performed LD immediately

[1] downloadable at `http://www.ti.com/lit/gpn/cc2420`

without executing RT and TPC. The RMD in the IDRS managed to effectively classify the interference as shown in class I, II, and III in Table 4. The total number of responses performed by IDRS is significantly less than the M_{TPC} and thus more energy efficient.

Table 3. The performance on the reliability (PDR), efficiency (TO) and energy usage (CC) for NST, MPR, M_{TPC} and IDRS under difference sources of interference

Radio Conditions	NST			MRP			M_{TPC}			IDRS		
	PDR (%)	TO	CC (mA)	PDR (%)	TO	CC (mA)	PDR (%)	TO	CC (mA)	PDR (%)	TO	CC (mA)
Normal	93.8	3.66	26.2	98.3	3.56	**25.9**	98.1	3.50	26.5	**98.4**	**3.49**	26.1
Class I	70.9	8.79	74.7	80.6	7.51	63.9	**84.9**	7.08	60.2	82.1	**6.55**	**55.7**
Class II	82.3	14.13	49.1	93.7	4.16	33.1	**96.9**	3.90	31.6	96.3	**3.78**	**31.0**
Class III	76.1	8.79	128.2	79.4	7.50	97.9	**87.1**	5.75	89.3	86.6	**5.36**	**83.6**

From Table 3, by increasing the transmission power as one of the response during Class I interference has improved the PDR by 5% on average compared to M_{TPC}. Although both M_{TPC} and IDRS exhibit similar PDR, IDRS has performed TPC less frequent than M_{TPC} during Class III error as Class I interference has been correctly classified by RDM as shown in Table 4 leading to better energy efficiency. Hence, the use of RDA to classify the radio signal noise pattern has not only allowed the system to response accurately with minimal energy consumption, but has also maintained a higher PDR.

Table 4. The execution of different responses with the interference classification in the IDRS, and without in the M_{TPC}. Results show that IDRS managed to execute the right response compared to M_{TPC}. Class III interference has been correctly classified resulting in higher number of Global discovery and lower number of high power transmission.

Radio Condition	Number of Response Executed								Interference Detected		
	RT		LD		TPC		GD		Class I	Class II	Class III
	IDRS	M_{TPC}	IDRS	M_{TPC}	IDRS	M_{TPC}	IDRS	M_{TPC}			
Normal	41	44	24	35	5	7	50	48	7	0	0
Class I	*113*	*174*	*52*	*92*	*33*	*12*	*342*	*404*	**59**	4	1
Class II	42	66	15	14	6	14	88	60	35	**15**	1
Class III	**164**	**193**	**108**	**145**	**15**	**44**	**121**	**219**	88	74	**82**

5 Conclusions

In this paper, we have presented an immune-inspired interference detection and recovery system (IDRS). This system consists of the MPR detection module, the RDA Diagnostic Module, and the Radio Interference Response Module. In the RDM, we have extended the usage of the RDA to diagnose certain types of

interference. Our experimental results have demonstrated that RDA can effectively classify the interference based on the RSSI values. Together with the use of the MRP, an effective response to network anomalies due to interference can be achieved. The results show that the IDRS can improve the PDR by 11% and reduce the energy consumption by 25.5% with Class I interference, and 10.5% improvement in PDR and saving of 34.8% in energy with Class III interference. It can also be used to detect anomalies that affecting the mote's radio. As the signature of normal RSSI can be easily regenerated as required, the IDRS can be made to adapt to its changing environment. As future work, we will incorporate an adaptive tunable activation threshold based on its environment and performance.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: A survey. Computer Networks 38(4), 393–422 (2002)
2. Boers, N., Nikolaidis, I., Gburzynski, P.: Patterns in the RSSI traces from an indoor urban environment. In: The IEEE International Workshop on Computer Aided Modeling, Analysis and Design of Communication Links and Networks, pp. 61–65 (2010)
3. Cohen, I.R.: Tending Adam's Garden: Evolving the Cognitive Immune Self. Academic Press (2004)
4. Drozda, M., Bate, I., Timmis, J.: Bio-inspired error detection for complex systems. In: The 17th IEEE Pacific Rim International Symposium on Dependable Computing, pp. 154–163 (2011)
5. Drozda, M., Schaust, S., Szczerbicka, H.: AIS for misbehavior detection in wireless sensor networks: Performance and design principles. In: The IEEE Congress on Evolutionary Computation, pp. 3719–3726 (2007)
6. Gomez, C., Salvatella, P., Alonso, O., Paradells, J.: Adapting AODV for IEEE 802.15.4 mesh sensor networks: Theoretical discussion and performance evaluation in a real environment. In: The IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks, pp. 159–170 (2006)
7. Hilder, J., Owens, N., Hickey, P., Cairns, S., Kilgour, D., Timmis, J., Tyrrell, A.: Parameter Optimisation in the Receptor Density Algorithm. In: Liò, P., Nicosia, G., Stibor, T. (eds.) ICARIS 2011. LNCS, vol. 6825, pp. 226–239. Springer, Heidelberg (2011)
8. Kim, J., Bentley, P., Wallenta, C., Ahmed, M., Hailes, S.: Danger Is Ubiquitous: Detecting Malicious Activities in Sensor Networks Using the Dendritic Cell Algorithm. In: Bersini, H., Carneiro, J. (eds.) ICARIS 2006. LNCS, vol. 4163, pp. 390–403. Springer, Heidelberg (2006)
9. Ko, J., Terzis, A.: Power control for mobile sensor networks: An experimental approach. In: The 7th Annual IEEE Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Networks (2010)
10. Lau, H.K., Timmis, J., Bate, I.: Collective Self-detection Scheme for Adaptive Error Detection in a Foraging Swarm of Robots. In: Liò, P., Nicosia, G., Stibor, T. (eds.) ICARIS 2011. LNCS, vol. 6825, pp. 254–267. Springer, Heidelberg (2011)
11. Lim, T.H., Bate, I., Timmis, J.: Multi-modal routing to tolerate failures. In: The 7th International Conference on Intelligent Sensors, Sensor Networks and Information Processing, pp. 211–216 (2011)

12. Lin, S., Zhang, J., Zhou, G., Gu, L., Stankovic, J., He, T.: ATPC: adaptive transmission power control for wireless sensor networks. In: The 4th International Conference on Embedded Networked Sensor Systems, pp. 223–236 (2006)
13. Lin, S., Zhou, G., Whitehouse, K., Wu, Y., Stankovic, J., He, T.: Towards stable network performance in wireless sensor networks. In: The 30th IEEE Real-Time Systems Symposium, pp. 227–237 (2009)
14. Liu, H., Li, J., Xie, Z., Lin, S., Whitehouse, K., Stankovic, J.A., Siu, D.: Automatic and robust breadcrumb system deployment for indoor firefighter applications. In: The 8th International Conference on Mobile Systems, Applications, and Services, pp. 21–34 (2010)
15. Owens, N., Greensted, A., Timmis, J., Tyrell, A.: T Cell Receptor Signalling Inspired Kernel Density Estimation and Anomaly Detection. In: Andrews, P.S., Timmis, J., Owens, N.D.L., Aickelin, U., Hart, E., Hone, A., Tyrrell, A.M. (eds.) ICARIS 2009. LNCS, vol. 5666, pp. 122–135. Springer, Heidelberg (2009)
16. Perkins, C.E., Royer, E.M.: Ad-hoc on-demand distance vector routing. In: The IEEE Workshop on Mobile Computing Systems and Applications, pp. 90–100 (1999)
17. Schaust, S., Szczerbicka, H.: Applying Antigen-Receptor Degeneracy Behavior for Misbehavior Response Selection in Wireless Sensor Networks. In: Liò, P., Nicosia, G., Stibor, T. (eds.) ICARIS 2011. LNCS, vol. 6825, pp. 212–225. Springer, Heidelberg (2011)
18. Wang, Y., Wang, Q., Zeng, Z., Zheng, G., Zheng, R.: Wicop: Engineering wifi temporal white-spaces for safe operations of wireless body area networks in medical applications. In: The IEEE International Real-Time Systems Symposium, pp. 170–179 (2011)
19. Wu, Y., Kapitanova, K., Li, J., Stankovic, J., Son, S., Whitehouse, K.: Run time assurance of application-level requirements in wireless sensor networks. In: The 9th ACM/IEEE International Conference on Information Processing in Sensor Networks, pp. 197–208 (2010)

Appendix: The Algorithm

input : Packet Send P_s
output: Response Action

```
while Packet Buffer is not Empty do
    Send Packet P_s and wait for acknowledgement P_ack;
    if P_ack is not received then                                  } Activate MRM
        Calculate Packet Sending Ratio, PSR                        } Detection
    else                                                           } Module.
        Decrease the cost for Retransmission, RT_cost;
    end
    if PSR < 95% then                                              } Activate RDA
        Determine interference CLASS from RDM;                     } Diagnostic
    end                                                            } Module.
    if not CLASS III and [PSR > 90% or RT_cost < RT_max] and
    Route is valid then                                            } Trigger
        Retransmit;                                                } Retransmission
        Increase the cost for Retransmission, RT_cost;             } Response.
    else if CLASS II and LD_cost < LD_max then                     }
        Perform Route Discovery;                                   } Trigger
        Increase the cost for Local Discovery LD_cost ;            } Local Discovery
        if Route Discovery is Successful then                      } Response.
            Decrease the cost of Retransmission RT_cost;           }
        end                                                        }
    else if CLASS I and Tx_Power < Tx_MAX then                     } Trigger Higher
        Increase the Transmission power, Tx_power;                 } Transmission
        Decrease the Retransmission Cost, RT_cost;                 } Power Response.
    else                                                           } Trigger
        Invalidate Route and Send Error for Global Discovery;      } Global Discovery
    end                                                            } Response.
    if Timeout then
        Reinitialised
    end
end
```

Algorithm 1: IDRS Algorithm with the combination of MRP and RDA