Detection of Dumb Nodes in a Stationary Wireless Sensor Network

Arijit Roy
Student Member, IEEE
School of Information Technology
IIT Kharagpur, India
arijitr@sit.iitkgp.ernet.in

Pushpendu Kar
Student Member, IEEE
School of Information Technology
IIT Kharagpur, India
pkar@sit.iitkgp.ernet.in

Sudip Misra
Senior Member, IEEE
School of Information Technology
IIT Kharagpur, India
smisra@sit.iitkgp.ernet.in

***Abstract*—A sensor node is termed as "dumb" [1], if at a certain time instant it can sense its surroundings, but is unable to communicate with any of its neighbors due to the shrinkage in communication range. Such isolation occurs because of the presence of adverse environmental effects. However, the node starts its normal operation with the resumption of favorable environmental conditions. Thus, the detection of dumb nodes is essential in order to re-establish network connectivity. However, the temporal behavior of a dumb node in a network makes the detection of such a node challenging. In the present work, we address a plausible solution to this problem by taking into account the evidences from neighboring nodes.**

***Index Terms*—Dumb Node, Environmental Effect, Detection, Evidence Theory.**

I. Introduction

THE rapid development of Micro-Electro-Mechanical Systems (MEMS) technology makes Wireless Sensor Networks (WSNs) economical. Presently, WSNs are widely used in a wide array of applications such as surveillance, target-tracking, health monitoring, and wild-life monitoring. Sensor nodes are deployed to sense data from a region of interest in a distributed manner and transmit those to a centralized unit through single or multi-hop connectivity [2], [3]. Thus, active participation and collaboration of each of the nodes is inevitable, so that the expected services from the network can be obtained. However, due to the resource constraint nature of WSNs, the nodes are vulnerable to environmental effects, Denial of Service (DoS) attacks and misbehavior. In order to protect the nodes from different vulnerabilities such as the ones mentioned above, different schemes have been proposed.

In the presence of adverse environmental conditions such as rainfall, temperature, and fog, a sensor node can sense its surroundings, but is unable to transmit the sensed information to the other nodes. This disruption of communication is temporary in nature. However, with the resumption of favorable environmental conditions a node can perform its normal operations. This temporary behavior of a node characterizes it to be *dumb* [1].

A. Motivation

Since the presence of dumb nodes impedes the overall network performance, their detection, and, subsequently, the re-establishment of network connectivity is crucial. Even in the presence of adverse environmental effects, dumb nodes can continue their sensing operation. However, communication with the other nodes is disrupted. The sensed information can only be utilized if the connectivity between each dumb node with other nodes in the network could be re-established. Before restoration of network connectivity, it is essential to detect the dumb nodes in the network. As dumb behavior is temporal in nature, their detection of dumb nodes is challenging. Existing methods proposed in the literature [4]–[6] were developed to handle misbehavior, attacks, and faults in a network. However, none of these is applicable for the detection of dumb nodes.

B. Contribution

In the present context, the dumb misbehavior [1] of sensor nodes is considered. In a WSN, collaboration among sensor nodes is crucial for the self-organization and proper functioning of the entire network. Like other misbehaviors of sensor nodes, dumb behavior also significantly degrades the network performance. We propose a new technique which is capable of identifying dumb nodes in a WSN so that the network can be restored to its normal working condition. The main *contributions* of the work are summarized as follows:

- This is an inaugural work on the identification of dumb nodes in a WSN. The proposed approach will be useful in situations in which communication within a network gets disrupted due to certain unfavorable environmental factors. This is because the network connectivity re-establishment algorithm should be executed only after the dumb nodes in the network are effectively recognized .
- The mathematical theory of evidence be Dempster Shafer Theory [7] is used in predicting the behavior (i.e., dumb or not) of each node in the network. The estimation procedure considers each node, one at a tim,e and takes into account the reward and penalty frequencies assigned to the current node by its neighboring nodes. Fusion of these statistical information from each of the neighboring nodes guarantees optimal prediction of the actual behavior of each node.
- A comprehensive theoretical justification, along with extensive experimental evaluation and analysis, emphasize

978-1-4799-5364-6/14/$31.00 ©2014 IEEE

potential applicability of the method in detecting dumb nodes in aWSN.

The rest of the paper is organized as follows. Section II gives an overview of the relevant work present in the existing literature. Section III-A highlights the primary objectives of the proposed work. Intrinsic characteristics of dumb nodes are explained in Section III-B. Section III-C describes the system model used in the work. An elaborate discussion of the proposed solution is given in Section IV. Section V provides the design issues and simulation parameters involved in the evaluation of the proposed method. Detailed analysis of results is presented in Section V-B. Concluding remarks of the work are finally given in Section VI.

II. Related Work

Our work is motivated by various faults and misbehavior in WSNs. Different issues related to faults, misbehavior, and attacks have been considered in the existing literature. Chen *et al*. presented an approach for detecting malicious behavior of a node by combining Monitor Group (MG) and routing table information in [8]. Another work proposed by Soltanmohammadi *et al*. in [9] is capable of detecting malicious nodes using a binary hypothesis testing framework. In this work, the honest node transmits binary decision to the fusion center, whereas a malicious node transmits fictitious messages to the fusion center and finally the fusion center helps in identifying the misbehaving nodes. An analytical framework for quantifying the impact of energy misbehavior on other nodes is given in [10], which focuses on both the individual nodes' as well as joint nodes' power optimization. A Group-based Trust Management Scheme (GTMS) is developed in [11] which prevents the path containing malicious, selfish, and faulty nodes. The proposed scheme uses a hybrid trust management approach that works with less communication overhead and uses less memory. Rajasegara *et al*. [12] provide an elaborate description of the different types of anomalies which may occur in a WSN and model these using statistical parameters on real data. The analytical results given in [12] report optimal strategies which facilitate the reduction in communication overhead. A light weight scheme proposed by Kamal *et al*. in [6] named as Sequence-based Fault Detection (SBFD) enables the detection of fault in a WSN. Fletcher checksum is used in tagging the network packets which are next delivered to the sink where network failure can be detected. A cluster-based hierarchical trust management scheme for WSNs was proposed by Bao *et al*. [4]. Liu *et al*. proposed an attacker detection scheme using spatial correlation for a large sensor network [5]. In this scheme, an attacker can be detected even without having any prior knowledge about the nodes. Environmental impact causes disruption in communication. The factors responsible for link breaking among nodes are temperature, rainfall, and fog. Boano *et al*. show how the communication is affected by temperature with real outdoor sensor deployment [13]. Due to the presence of such environmental impact on the sensor nodes, the communication range of a node gets reduced, and consequently, the sensor nodes get dumb [1]. Existing approaches to detection of malicious or selfish nodes in the literature are not suitable for detecting dumb nodes.

III. Problem Description

A. Objectives

In a WSN, the sensor nodes communicate using multi-hop connectivity. The communication range of a node decreases dynamically with the change in environmental conditions. When the communication range of a particular node is less than the distance to its nearest active neighbor node, it cannot transmit any data to its neighbor nodes. Consequently, the node becomes dumb. In such a scenario, it is required to re-establish connectivity among all the nodes in the network. The connectivity re-establishment algorithm, in turn, requires knowledge about the dumb nodes present in the network. The objective of the proposed scheme is to detect all the dumb nodes in the network, so that a centralized unit or the dumb nodes can start re-establishing network connectivity.

B. Dumb Nodes

In this work, we assume that each sensor node in the network is homogeneous, i.e., each node has the same capability of sensing and transmitting.

Definition 1. *Dumb Behavior: A sensor node that can sense physical phenomena in its surroundings, and cannot transmit the sensed data at a certain instant of time due to presence of adverse environmental condition, but transmit at a later instant, with the resumption of favorable environmental condition, is termed as a dumb node. Such behavior is denoted by Ψ_d. Mathematically* [1],

$$\Psi_d = \begin{cases} 1, & \{(0 < d_{min} \le r_c(t_i) \le R)\} \\ & \wedge\{0 \le r_c(t_j) < d_{min} < R)\} \quad \forall t_i, t_j \quad t_i \neq t_j \\ 0, & otherwise \end{cases}$$

Fig. 1, exhibits the occurrence of dumb node A. As shown in the Figure (a), the distance between A and its nearest active neighbor node is denoted by d_{min}. The communication range of node A at time instant t_i is $r_c(t_i)$, but at a later instant of time t_j as shown in Figure (b), the communication range of node A shrinks and becomes $r_c(t_j)$, which is less than d_{min}. Thus, due to this shrinkage in communication range,

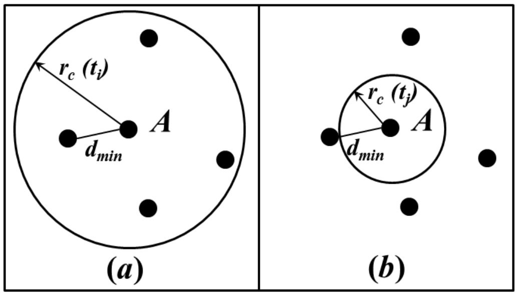

Fig. 1: Dumb node

node A fails to transmit any data packet at time instant t_j to any activated neighbor node and it becomes dumb.

Definition 2. *Major Block (MB): The whole terrain is divided into four equal parts each of which is termed as a* Major Block. *Such a design enables each individual* Mobile Agent *to monitor the terrain simultaneously, thereby saving significant processing time.*

Definition 3. *Mobile Agent (MA): A Mobile Agent is a sensor node which gathers the required information from other sensor nodes within its MB and transmits it to the sink. The functionality of a mobile agent is similar to that of any sensor node. But it is capable of recharging itself, i.e., there is no any power constraint.*

C. System Model

Let us consider a collection of GPS-enabled sensor nodes deployed over a terrain. Among these few are activated so that the terrain can be covered completely. Each of the sensor nodes has an unique id and broadcasts a periodic $HELLO$ message with an assigned sequence number. The $HELLO$ message broadcasted from a node informs its neighbor nodes about the existence in the network. The packet format of a $HELLO$ message is shown in Fig.2. The system is modeled as a graph $G(N, L)$, where N is the set of nodes and L is set of links. A node n_i is connected with another node n_j through link l_{ij}, where, n_i, $n_j \in N$ and $l_{ij} \in L$. In the proposed model, each neighbor node of a node n assigns a reward on getting a $HELLO$ message from other nodes. For determining the reward, we use a parameter termed as *Reward Indicator* R. This parameter value is set to 1 on receiving a $HELLO$ message from the neighbor nodes of n, whereas it is set to 0 if no $HELLO$ message is received. To be more specific, if a neighbor node of n receives a $HELLO$ message out of sequence, it assumes that the missing $HELLO$ message is not received due to the shrinkage in communication range of n, and accordingly a penalty is assigned.

1byte	1byte	4bytes
type	***seq_no***	***src_id***

Fig. 2: Packet format of $HELLO$ message

$$R = \begin{cases} 1, & \text{if } HELLO \text{ message is received} \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

Similarly, *Penalty Indicator* P is used to determine the penalty.

$$P = \begin{cases} 1, & \text{if } HELLO \text{ message is not received} \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

As explained in Section III-B, dumb behavior is dynamic in nature. This temporal behavior of node is observed for a period of time, and thereafter, the reward and penalty of the node is computed with the help of *exponential moving average*. Such an averaging scheme considers the history of the node and accordingly determines the reward and penalty.

Definition 4. *Time Gap: The time difference between two consecutive $HELLO$ messages is called the Time Gap (T_G). Mathematically:*

$$T_G = (T_x - T_y) \tag{3}$$

where T_x and T_y are the time instances of broadcasting $HELLO$ messages H_n and H_{n+1}, respectively.

Definition 5. *Vulnerable Time: The Vulnerable Time T_V is defined as the sum of the maximum time duration (T_p) for propagating a $HELLO$ message and the time (T_a) required to receive acknowledgment against this message. Mathematically:*

$$T_V = T_p + T_a \tag{4}$$

Definition 6. *Discarding Factor (α): The Discarding Factor (α), depends on T_G. In our system, α is inversely proportional to T_G, i.e., a higher value of T_G, produces a lower value of α. Mathematically, α is represented as:*

$$\alpha = \frac{T_V}{T_G}. \tag{5}$$

α is a coefficient such that $0 \leq \alpha \leq 1$. A greater value of α results in the decrement of the older value of the reward at a faster rate. More emphasis is given to the previous history if the number of $HELLO$ messages is less per unit time. Consequently, the value of α is derived in term of T_G.

The sensor nodes are deployed and are expected to receive $HELLO$ messages successfully from their respective neighbors after a certain interval of time. Therefore, r_0 is assumed to be 1. For the same reason, p_0 must be assigned a value of 0.

With the help of the exponential moving average, the reward and penalty for a particular node n, after time instant t, is given as:

$$\begin{aligned} r_0 &= R_0^n \\ r_t^n &= \alpha R_t^n + (1-\alpha) r_{t-1} \end{aligned} \tag{6}$$

$$\begin{aligned} p_0 &= P_0^n \\ p_t^n &= \alpha P_t^n + (1-\alpha) p_{t-1} \end{aligned} \tag{7}$$

Lemma 1. *The maximum and the minimum values of reward are 1 and $(1 - \alpha)$, where α is the discarding factor.*

Proof. The reward function id is given by:

$$r_t = \alpha R_t + (1-\alpha) r_{t-1} \tag{8}$$

We have,

$$\begin{aligned} r_{t-1} &= [\alpha R_t + (1-\alpha) r_{t-2}] \\ &= \alpha R_t + (1-\alpha)[\alpha R_t + (1-\alpha) r_{t-2}] \end{aligned} \tag{9}$$

Similarly, we have,

$$\begin{aligned} r_t = \alpha[R_t + (1-\alpha)R_{t-1} + (1-\alpha)^2 + R_{t-2} + \cdots + \\ (1-\alpha)^{t-1} R_1 + (1-\alpha) r_{t-2}] + (1-\alpha)^t r_0 \end{aligned} \tag{10}$$

Algorithm 1 Dumb node detection

```
Inputs:
$n_i \leftarrow i^{th}$ active node, $[i = 1, 2, 3, \cdots, N_A]$, where, $N_A$ is the total number of active nodes
$\mathcal{N}(n_i) \leftarrow$ neighbor list of the $i^{th}$ active node
$\mathcal{N}_j(n_i) \leftarrow j^{th}$ neighbor of the $i^{th}$ active node   $[j = 1, 2, 3, \cdots, \mathcal{N}(n_i)]$
$\alpha \leftarrow$ discarding factor

Output:
Predict if node $n_i$ is dumb

Begin
1.  Each $n_i$ broadcasts $HELLO$ message at time $t$,   $[t = 1, 2, 3, \cdots, T]$
2.  For $t$ = 1 to $T$
3.     For $j$ = 1 to $\mathcal{N}_j(n_i)$
4.        if $\mathcal{N}_(n_i)$ receives $HELLO$ message
       //assign reward $(R_{j,t})$ and penalty $(P_{j,t})$ value accordingly
5.           $R_{j,t} \leftarrow 1$
6.           $P_{j,t} \leftarrow 0$
6.        Else
7.           $R_{j,t} \leftarrow 0$
8.           $P_{j,t} \leftarrow 1$
9.        End if
       //update penalty and reward
10.         $p_{j,t} \leftarrow \alpha P_{j,t} + (1-\alpha)p_{1,(t-1)}$
11.         $r_{j,t} \leftarrow \alpha R_{j,t} + (1-\alpha)r_{1,(t-1)}$
12.       End For
13.   End For
14. $m(B) \leftarrow r_{1,t}/(p_{1,t} + r_{1,t} + 2)$   //combined belief for node $n_i$
15. $m(D) \leftarrow p_{1,t}/(p_{1,t} + r_{1,t} + 2)$   //combined disbelief for node $n_i$
16. $m(U) \leftarrow 2/(p_{1,t} + r_{1,t} + 2)$   //combined uncertainty for node $n_i$
17. For $j$ = 2 to $\mathcal{N}(n_i)$
18.     $m(B) \leftarrow m(B) \oplus r_{j,t}/(p_{j,t} + r_{j,t} + 2)$
19.     $m(D) \leftarrow m(D) \oplus p_{j,t}/(p_{j,t} + r_{j,t} + 2)$
20.     $m(U) \leftarrow m(U) \oplus 2/(p_{j,t} + r_{j,t} + 2)$
21. End For
22.  if $m(B) \geq m(D)$
23.     node $n_i$ is not dumb
24.  Else
25.     node $n_i$ is dumb
26.  End If
End
```

In the i^{th} step,

$$r_t = \sum_{i=0}^{t-1}(1-\alpha)^i R_{t-i} + (1-\alpha)^t r_0 \qquad (11)$$

If we consider $r_0 = 1$ and $R_i = 0,\ 1 \leq i \leq t$
We have,

$$(r_t)_{min} = (1-\alpha)^t \qquad (12)$$

Again, if we consider $r_0 = 1$ and $R_i = 1,\ \forall i \leq t$

$$\begin{aligned} (r_t)_{max} &= \alpha \sum_{i=0}^{t-1}(1-\alpha)^i + (1-\alpha)^t \\ &= \alpha \frac{1-(1-\alpha)^t}{1-(1-\alpha)} + (1-\alpha)^t \end{aligned} \qquad (13)$$

$$(r_t)_{max} = 1 \qquad (14)$$

□

After fixed intervals of time, MA collects the reward and penalty from each of the nodes in its MB. Let us consider a certain node n in the network and suppose it has a total of K neighbors. Let us denote the reward and penalty values assigned by the k^{th} neighbor of the node n after time t to be r_k^n and p_k^n where, $k = 1, 2, 3, \cdots, K$. The belief, disbelief, and uncertainty parameters of the node corresponding to its k^{th} neighbor are denoted by b_k^n, d_k^n, and u_k^n respectively. MA computes b_k^n, d_k^n, u_k^n using the set of reward and penalty values following the beta reputation model [14], [15] given by:

$$b_k^n = \frac{r_k^n}{r_k^n + p_k^n + 2} \qquad (15)$$

$$d_k^n = \frac{p_k^n}{r_k^n + p_k^n + 2} \qquad (16)$$

$$u_k^n = \frac{2}{r_k^n + p_k^n + 2} \qquad (17)$$

IV. Node behavior identification

A. Dempster Shafer Theory

The penalties and rewards assigned by the neighbors of a certain node are used in deriving the belief, disbelief and uncertainty evidence values. *Dempster Shafer Theory* (DST) [7] is, henceforth, used to fuse these evidences together for making a final prediction about the behavior of the node, as shown in Steps 14-26 of Algorithm 1.

Let θ be the finite set of mutually exclusive and exhaustive hypotheses for a system. θ is called *frame of discernment*. A basic belief assignment (BBA) or mass function [7] is defined by $m : 2^\theta \rightarrow \{b, d\}$, such that:

$$m(\phi) = 0 \qquad (18)$$

$$\sum_{A \subseteq \theta}(A) = 1 \qquad (19)$$

B. Frame for dumb node detection

Let us consider a certain node n. For this node θ is $\{b, d\}$. The power set of discernment is given by:

$$2^\theta = \{\phi, b, d, u\} \qquad (20)$$

where $u = \{b \cup d\}$.

For combining the set of evidences from the neighboring nodes, DST is applied. On the basis of the strengths of the evidences given by the individual neighbor nodes of n, DST decides whether the node n is dumb or not. Let $m_1(x)$ and $m_2(x)$ be the masses of independent sets of observations for evidence x, $(x \in \{b,\ d,\ u\})$ computed from two different neighbor nodes of n after a time instant t. These pieces of information can be fused together with the help of the rule of combination of DST to give the combined mass $m(X)$, where

$$m(X) = m_1(x) \oplus m_2(x). \qquad (21)$$

The combined mass for belief (b) can be computed as follows:

$$m_1(b) \oplus m_2(b) = \frac{\sum\limits_{b,d:b \cap d = x} m_1(b).m_2(b)}{1 - \sum\limits_{b,d:b \cap d = \phi} m_1(b).m_2(b)} \qquad (22)$$

Equation 22 can be extended for any number of neighboring nodes. For k neighbors, the combined strength of belief $m(B)$ is given by:

$$m(B) = m_1 \oplus m_2 \oplus m_3 \oplus \cdots \oplus m_k. \qquad (23)$$

The combined mass for disbelief can also be computed similarly. The final decision is taken depending on the magnitudes

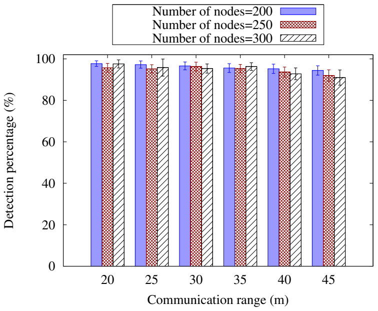

Fig. 3: Percentage of detection

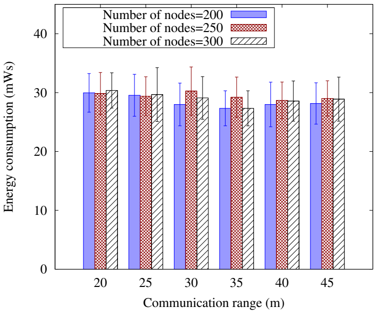

Fig. 4: Energy consumption

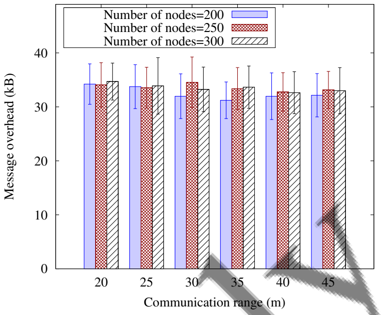

Fig. 5: Message overhead

of $m(B)$ and $m(D)$. If $m(B) < m(D)$, the node n is said to be dumb and vice-versa.

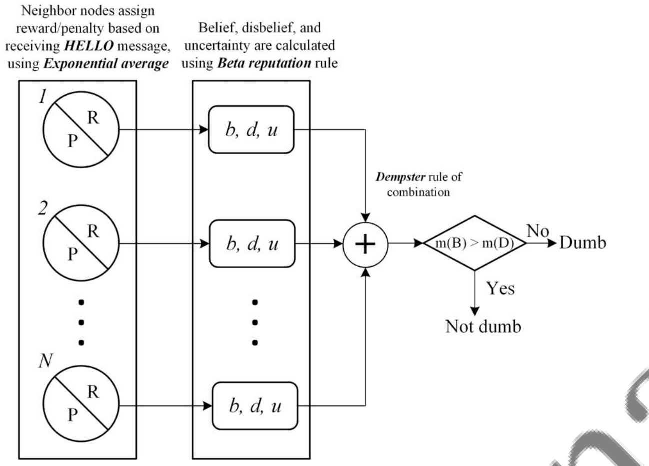
Neighbor nodes assign reward/penalty based on receiving HELLO message, using Exponential average
Belief, disbelief, and uncertainty are calculated using Beta reputation rule
1
R
P
b, d, u
2
R
P
b, d, u
N
R
P
b, d, u
Dempster rule of combination
+
m(B) > m(D)
No
Dumb
Yes
Not dumb

Fig. 6: A schematic diagram of dumb node detection system

Fig. 6 shows the schematic diagram of the proposed system used for dumb node detection. As seen in the figure, there are total N nodes present in the system, each of which computes the penalty and reward values corresponding to all the nodes from which they receive the $HELLO$ messages after fixed time intervals of T_G. Using these penalty and reward values, the magnitudes of b, d, u are next determined. Once MA gathers the information from all of the neighbor nodes, it applies the Dempster rule of combination given in Equation 23, and takes a final decision about the behavior of the node, as shown in Fig. 6.

Algorithm 1 depicts our proposed scheme of dumb node detection in a WSN.

V. Performance Evaluation

A. Simulation Design

In this section, we evaluate the performance of the proposed algorithm for the detection of dumb nodes in a WSN. Further, this behavior is temporal in nature. In the existing literature there does not exist any method for the detection of dumb nodes. Hence, comparative analysis with related work is out of scope. The list of simulation parameters used is shown in Table I. We considered total of $200 - 300$ nodes deployed randomly. A set of nodes is activated which can cover the entire simulation region, while the rest of the nodes remain in the sleep mode. All the sensor nodes have the same capability of sensing and transmitting. Each node broadcasts a $HELLO$ message periodically. The size of the $HELLO$ message is 6 bytes, as shown in Fig. 2. However, for verifying the effectiveness of the proposed approach, we carry out extensive experimentation considering the following parameters:

- *Detection percentage*: The percentage of dumb nodes detected by our scheme
- *Energy consumption*: The energy required to detect dumb nodes (measured in $milliWattsecond$ (mWs))
- *Message overhead*: Total amount of control message required to detect dumb nodes (measured in $kiloBytes$ (kB))

TABLE I: Simulation Parameters

Parameter	Value
Number of nodes	200-300
Simulation area	500 m × 500 m
Sensing range	25 m
Communication range	20-60 m
Data rate	250 kbps

Energy consumption model: The proposed algorithm uses the same energy consumption model for transmitting a packet of N bits from one sensor node to another at a constant data rate R [16], [17], which is given by:

$$E_T(d) = \frac{P_T \times N}{R} \tag{24}$$

B. Results

Fig. 3 depicts the performance of the proposed algorithm when used to detect dumb nodes with varying communication range. The communication range varies between $20 - 45$ m and is plotted along the X axis, whereas the detection percentage is plotted along the Y axis. As seen in the figure, for a given value of the communication range, three different settings for the total number of nodes is considered. In our simulations, we consider the total number of nodes to be 200, 250 and 300, respectively. In each of the cases the detection percentage is more than 90%. Figs. 4 and 5, respectively, represent the energy consumption and overhead in the network while detecting dumb nodes. Fig. 4 shows the variation in

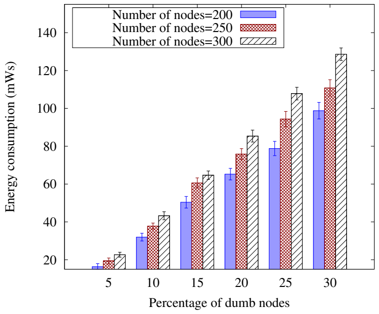

Fig. 7: Energy consumption with percentage of dumb nodes

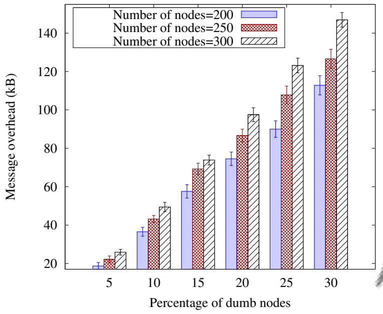

Fig. 8: Message overhead with percentage of dumb nodes

the energy consumption with increase in the communication range. It can be seen from the plot that energy consumption attains the maximum limit of 32 *mWs*. Again, in Fig. 5, it can be seen that the message overhead in each of the cases is less than 40 *kB*.

Fig. 7 depicts the plot of the energy consumption with variation in the percentage of the number of dumb nodes. In this figure, the percentage of dumb nodes is plotted along the X axis with an interval of 5% up to 30%. It is observed that with the increase in the percentage of dumb nodes, the energy consumption for detection also increases. Fig. 8 shows the total overhead incurred in detecting dumb nodes. In this figure, we can observe that there is a steady increase in the message overhead as the percentage of dumb nodes increases.

VI. Conclusion

In this work, we have proposed a scheme for the detection of dumb nodes in a WSN. In such a network, the dumb behavior of a node occurs due to the shrinkage in communication range in the presence of adverse environmental effects. As dumb behavior is temporal in nature, its detection is significantly challenging. We propose an approach to detect dumb nodes with the help of mobile agent taking into account the evidences from the neighbor nodes of a dumb node. The simulation results show the effectiveness of the proposed scheme of dumb node detection. The detection scheme can be further extended for distributed approach.

In the future, we plan to extend our work by detecting dumb nodes using social choice theory in order to consider the opinion of neighbor nodes of a dumb node.Thereafter, establishing network connectivity between the dumb node and other nodes. Another approach we plan to explore for detecting dumb nodes is using Markov chain analysis of a nodes state.

References

[1] S. Misra, P. Kar, A. Roy, and M. S. Obaidat, “Existence of dumb nodes in stationary wireless sensor networks,” *Journal of Systems and Software*, vol. 91, pp. 135–146, May 2014.

[2] I. F. Akyildiz, S. Weilian, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” *Communications Magazine*, vol. 40, no. 8, pp. 102–114, November 2002.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[4] F. Bao, I.-R. Chen, M.-J. Chang, and J.-H. Cho, “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection,” *IEEE Transaction on Network and Service Management*, vol. 9, no. 2, pp. 169–183, June 2012.

[5] F. Liu, X. Cheng, and D. Chen, “Insider attacker detection in wireless sensor networks,” in *INFOCOM*, May 2007, pp. 1937–1945.

[6] A. R. M. Kamal, C. J. Bleakley, and S. Dobson, “Failure detection in wireless sensor networks: A sequence-based dynamic approach,” *ACM Transactions on Sensor Networks*, vol. 10, no. 2, pp. 35:1–35:29, January 2014, article No 35.

[7] M. Ahmed, X. Huang, D. Sharma, and L. Shutao, “Wireless sensor network internal attacker identification with multiple evidence by dempster-shafer theory,” in *Proceedings of the* 12^{th} *International Conference on Algorithms and Architectures for Parallel Processing*, Berlin, Heidelberg, 2012, pp. 255–263.

[8] R.-C. Chen, C.-F. Hsieh, and Y.-F. Huang, “A new method for intrusion detection on hierarchical wireless sensor networks,” in *3rd International Conference on Ubiquitous Information Management and Communication*, 2009, pp. 38–45.

[9] E. Soltanmohammadi, M. Orooji, and M. Naraghi-Pour, “Decentralized hypothesis testing in wireless sensor networks in the presence of misbehaving nodes,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 205–215, January 2013.

[10] R. Kannan, S. Wei, V. Chakravarthi, and G. Seetharaman, “Analysis of communication vulnerability through misbehavior in wireless and sensor networks,” in *Military Communications Conference*, October 2005, p. 10401046.

[11] R. A. Shaikh, H. Jameel, B. J. dAuriol, H. Lee, S. Lee, and Y.-J. Song, “Group-based trust management scheme for clustered wireless sensor networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 11, pp. 1698–1712, November 2009.

[12] S. Rajasegarar, J. C. Bezdek, C. Leckie, and M. Palaniswami, “Elliptical anomalies in wireless sensor networks,” *ACM Transactions on Sensor Networks*, vol. 6, no. 1, pp. 7:1–7:28, December 2009, article 7.

[13] N. T. C A Boano, T. Voigt, J. Brown, and U. Roedig, “The impact of temperature on outdoor industrial sensornet applications,” *IEEE Transactions on Industrial Informatics*, vol. 6, no. 3, pp. 451–459, August 2010.

[14] A. Jsang, “A logic for uncertain probabilities,” *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 9, no. 3, pp. 279–311, June 2001.

[15] A. Jsang and R. Ismail, “The beta reputation system,” in *Proceedings of the 15th Bled Electronic Commerce Conference e-Reality: Constructing the e-Economy*, June 2002, pp. 1–14.

[16] S. Misra, G. Mali, and A. Mondal, “Distributed topology management for wireless multimedia sensor networks: exploiting connectivity and cooperation,” *International Journal of Communication Systems (Wiley)*, vol. 27, no. 3, March 2014.

[17] Q. Wang, H. Mark, and Y. Woodward, “A realistic power consumption model for wireless sensor network devices,” in *Sensor and Ad Hoc Communications and Networks*, vol. 1. 3rd Annual IEEE Communications Society, 2006, p. 286295.