https://doi.org/10.1016/j.jss.2013.12.039

Existence of Dumb Nodes in Stationary Wireless Sensor Networks

Sudip Misra, Pushpendu Kar, Arijit Roy
School of Information Technology
Indian Institute of Technology Kharagpur
Kharagpur 721302, India
Email: {smisra, pkar, arijitr}@sit.iitkgp.ernet.in

Mohammad S. Obaidat
Fellow of IEEE, *Fellow of SCS*
Dept. of Computer Science and Software Enggineering
Monmouth University
West Long Branch, NJ. USA
Email: obaidat@monmouth.edu

Abstract

Wireless Sensor Networks (WSNs), which are typically autonomous and unattended, require energy-efficient and fault-tolerant protocols to maximize the network lifetime and operations. In this work, we consider a previously unexplored aspect of the sensing nodes – *dumb behavior*. A sensor node is termed as "dumb", when it can sense its surroundings, but cannot communicate with its neighbors due to shrinkage in communication range attributed to environmental effects and can behave normally in the presence of favorable environment. As a result of this temporary behavior, a node may get isolated from the network when environment effects are present, but re-connectes with the network with the resumption of favorable environmental conditions. We consider the effects of dumb nodes on the, otherwise, energy-efficient stationary WSNs having complete network coverage achieved using sufficient number of activated sensor nodes. While the presence of redundancy in the deployment of nodes, or the number of active nodes can guarantee communication opportunities, such deployment is not necessarily energy-efficient and cost-effective. The dumb behavior of nodes results in wastage of power, thereby reducing the lifetime of a network. Such effects can be detrimental to the performance of WSN applications. The simulation results exhibit that the network performance degrades in the presence of dumb nodes in stationary WSNs.

Index Terms

Wireless Sensor Networks; Energy Efficiency; Environmental Effects; Dumb Nodes.

I. Introduction

Advancement of tiny embedded devices has led to the development of low power, high performance, and cost effective sensor nodes. Due to the limited communication range of these nodes, the intermediate nodes act as relay ones to forward sensed information to the sink [1]. Sensor nodes orchestrate in a collaborative manner to measure their surrounding physical environment (i.e., light, pressure, temperature, humidity, and vibration). Due to the amelioration of sensor technology, the nodes offer functionalities in improved ways such as sensing the phenomena from larger distances, sensing accuracy, increased performance, and lower cost. However, in respect of power, there is limited noticeable advancement. So, research efforts on energy-efficient and fault-tolerant protocols [2], [3] to maximize network lifetime and operations have witnessed an up-surge. Apart from the energy aspects and other resource-constraint induced faults, the performance of WSNs may get affected by other factors such as environmental effects, denial of services, attacks, misbehaving, and faulty nodes. Such effects are detrimental to the performance of WSNs, especially those concerning critical applications such as surveillance [4] and target tracking [5]. However, one of the aspects that has been largely overlooked in the current literature is the effect of the existence of sensor nodes that can sense, but fail to communicate sensed data, due to shrinkage in communication range attributed to environmental factors. The sensor nodes are assumed to communicate through an obstacle-free medium, where signals get attenuated due to the presence of environmental effects. Shrinkage of communication range depends on intensity of adverse environmental effects. When the communication range of a sensor node decreases below a certain threshold, it cannot communicate any more with its neighbor nodes, which were previously within the communication range of that particular node. In such a scenario, connectivity is lost between the sensor nodes, and, thus, one or more sensor nodes get isolated from the network. As WSNs are energy-constrained, it is important to activate certain number of intermediate nodes, so that the connectivity that is lost between the nodes can be re-established, thereby causing increased energy consumption.

A. Motivation

As WSNs are typically unattended and autonomous, they are prone to faults, misbehavior, and external attacks. A faulty sensor node may not cover its sensing area, create congestion in the network [6] [7] drop its received packets, and, mis-route them. The possible effects of misbehavior of a sensor node include packet dropping, modification of routing information or packets, skewing of network topology, and creating fictitious node [8]. Here, we have considered a specific type of misbehavior, termed as "dumb" behavior, which, to the best of our knowledge, has not been considered explicitly in the existing literature. A node is termed as "dumb", if it can sense its surroundings, but cannot communicate with its neighbors due to the shrinkage in communication range attributed to the onset of environmental factors such as fog, rainfall, heat and can behave normally in the presence of favorable environmental conditions. Environmental effects are inherently not permanent, i.e., they are time-varying. Thus, a sensor node exhibiting dumb behavior in the presence of environmental effects is called as a *dumb node*. Dumb behavior can be considered as a serious misbehavior that can have detrimental effects on network performance, similar to other forms of misbehavior in WSNs. Therefore, it is imperative to identify and explore the different effects of a dumb node in WSNs.

B. Contributions

Following the deployment of sensor nodes, collaboration is a crucial factor for self-organization of the entire network, and for yielding good performance. Misbehavior is a serious issue that can pose as an obstacle in collaboration among sensor nodes.

The specific *contributions* in this paper are summarized below:

- Identifying a previously unexplored aspect of the sensor nodes – *dumb behavior*, which is inherently dynamic.
- Performance comparison between dumb, selfish, and dead nodes.
- Theoretical characterization of effects due to the presence of dumb nodes on the overall power consumption and transmission delay of WSNs.
- Simulation - based evaluation of the effects on the performance of WSNs in the presence of dumb, selfish, and dead nodes.

C. Organization

The rest of the paper is organized as follows. Section II describes the related work done in this area. Section III discusses the objective of the proposed work. Section IV defines a dumb node, and describes its characteristics. Section V presents the different effects induced due to the presence of dumb nodes in the network. We delineate a simulation design and analyze the results in Section VI. We conclude our work in Section VII.

II. Related Work

A number of works addressing misbehavior of nodes in sensor and related networks exist in the literature. Huangshui et al. [9] discussed the issue of malfunctioning of sensors arising due to several reasons such as environmental noise, interference, malicious attacks, and potential software bug. The authors, however, only considered nodes having faulty sensing behavior. They did not focus on nodes that can sense, but cannot communicate. In [10], Anastasi et al. showed how the performance of a sensor node is affected in the presence of environmental constraint. Environmental conditions is one of the major causes for permanent or temporary wireless link failure [11]. Temperature is also an issue affecting signal strength of communication link and transmission power of sensor nodes [12]–[14]. In [15] and [16], the authors explored connectivity issues associated with a low-cost environmental sensing network. They presented empirical data quantifying the propagation effects for three naturally occurring environments: open area, wooded area, wooded and hilly area. In [17], the authors adopted a two-level approach for developing a computational model based on life-cycle assessment (LCA) and energy modeling. They first explored WSN infrastructure and its life-cycle and presented environmental impact on the assessment model in detail. Dhurandher et al. [18] considered misbehaving node based on QoS and reputation to find secure path for routing. However, they did not consider nodes, which can sense but not communicate with neighbors as misbehaving node.

In [19], the authors discussed about the optimal uses of resources, and for this, the optimal number of neighbor nodes to be activated to form the back-bone of the entire network. However, if these neighbor nodes are dumb, the neighbor nodes cannot get activation requests, due to the shrinkage in communication range of a node. Yim et al. [20] discussed scenarios in which sensed data get modified due to malicious behaviors of sensor nodes. They proposed a malicious node detection scheme based on the reputation of the nodes with their neighbors. Ruiz et al. in [21] proposed and evaluated a failure detection scheme using a management architecture for WSNs, called MANNA. This can provide self-configuration, self-diagnostic, and self-healing, and some of the self-managing capabilities automatically to event-driven WSNs. A novel formulation of the problem of energy misbehavior is presented in [22]. The authors developed an analytical framework for quantifying its impact on other nodes. Their analytical results revealed optimal strategies for attacking nodes in an enemy network through energy depletion. Effective defense mechanisms for protecting their own wireless network against energy attacks by an intelligent adversary were also designed by them. However, their work overlooked the issue of a node being able to sense, but unable to communicate with their neighbors. In such a case, their proposed scheme may fail to determine the reputation due to lack of communication with neighbors. Paradis and Han [11] discussed the issue of existence of faults in sensor nodes. They identified link breakage fault permanently or temporarily blocked by an external object or due to environmental factors. For a particular node, all the links may not break with all its neighbors at the same time, and there may be some links to communicate. However, the authors overlooked the situation where all the links of a node are disconnected due to its dumb behavior. Khelifa et al. in [23], developed a new monitoring mechanism to guarantee strong connectivity in WSNs. This mechanism, at any time, detects the critical nodes that represent articulation points for monitoring sensor connectivity. These articulation points disconnect portions of the networks. Hence, they developed a mechanism for self-organization to increase the degree of connectivity in their vicinity, thereby increasing fault tolerance. However, the authors did not consider the environmental effect due to which a node can behave as dumb and the degree of connectivity due to dumb behavior is reducing. In [24], the authors studied coverage with connectivity properties in large WSNs. They considered three classes: full coverage with connectivity, partial coverage with connectivity, and constrained coverage with connectivity. Surveillance performance and deployment cost for networks with different coverage and connectivity criteria were compared by them. In [25], the authors discussed about connectivity issues on the basis of optimized deployment of target coverage. They first determined disconnected edges of connected subset using minimum spanning tree, and then constructed a connected candidate set. In all the above mentioned works, there may be a situation when there is complete coverage of the network, but partial connectivity may exist due to presence of dumb node in the network, which is, again, overlooked by these authors as well. In [26], Kamhoua et al. discussed three types of misbehaving nodes in a multi-hop wireless network – faulty, selfish, and malicious. Nodes, which do not obey the protocol, are faulty. Selfish nodes are those that do not communicate for saving their resources and malicious nodes are formed by various attacks. In [27], misbehavior is classified into three major categories: (a) a node exhibiting misbehavior but is not malicious, (b) a node eavesdropping and causing denial of service (DoS) in the network, and (c) malicious behavior due to compromise in a node. Dumb behavior can be classified into the first category.

With the intention of affecting the routing service in the network, a node may drop, modify or mis-route packets – known as Byzantine behavior [28]. When a single sensor node advertises multiple identities to the network, it is called impersonification. DoS attacks [29] are launched when the attacker tries to diminish or eliminate network capacity to perform its expected function. Selfishness is another type of misbehavior in which a sensor node forwards the packets sensed by itself, but does not forward those that are received from the other nodes, for preserving its energy and resources [30].

Soltanmohammadi et al. [31] discussed misbehavior caused due to hardware and software degradation. They identified different classes of nodes and estimated the operating point of each class and detected each of the misbehaving classes by formulating and solving the problem using expectation maximization algorithm. However, the authors has not considered the detection of misbehavior occur due to shrinkage of communication range by the environmental effect.

A review of the existing literature reveals different types of environmental effects that are considered. However, the works did not consider, which sensor nodes can sense, but may not be able to communicate with its neighbors, due to the presence of adverse environmental effects, but communicate when the environment becomes normal. Thus, the behavior is temporary in nature. This type of behavior of a node affects network performance with respect to throughput, delay, delivery ratio, energy consumption and lifetime of a network. In this work, we have characterized it as *dumb behavior*, and discussed the effects of this behavior on the overall performance of the network.

III. Objective

The presence of dumb nodes in the network requires serious attention due to environment-induced dynamically increasing or decreasing communication range. As mentioned earlier, a dumb node can sense physical phenomena, but cannot communicate the sense data with other nodes in its vicinity, temporarily. In this paper, we try to address the issues arising due to the existence of dumb nodes in a network. If one or more co-located sensor nodes start behaving dumb due to environmental reasons, then there is loss in connectivity between the nodes, which exhibits different types of communication problems, as mentioned in Section V. The dumb nature of a sensor node may be time varying, depending upon the environmental conditions, i.e., at a particular point of time it may exhibit dumb nature, while in the future it may not, and vice versa. In such a scenario, we have to measure network performance, considering different parameters in the network. Therefore, network partitioning and node isolation may not occur permanently due to the presence of dumb nodes. So, the network re-construction methodologies should adapt to such dynamic behavior.

TABLE I: Notation Table

Name	**Description**
R	Specified communication range
Ψ_n	Normal behavior
Ψ_d	Dumb behavior
d_{min}	Distance from a node to its nearest neighbor node
r_c^{ne}	Communication range of a node when it shrink up to neighbor node ne
ne	Neighbor node
$r_c(t)$	Communication range at time instant t
A	Area
N	Number of nodes
D_N	Node density
P_{dumb}	Probability that a node is dumb
N_{disk}	Number of nodes in a disk area
d	Distance between two nodes
N_{min}	Minimum number of nodes to be activated to establish re-connectivity
E_i	Intensity of the environmental effect
P	Power Consumption
P_T	Total power consumption
ΔR	Shrinkage in communication range
I_N	Number of nodes on the path between source and destination nodes
$L_C^{I_N}$	Link count from source to destination nodes, having I_N intermediate nodes
T_{path}	Time taken for path establishment
$T_{success}$	Time for successful packet delivery
$T_{unsuccess}$	Time for unsuccessful packet delivery
T	Total time taken for packet delivery when dumb node arise

IV. Dumb Nodes

A. *Dumb node in real life scenario*

The dumb nature of a sensor node arises due to temporary shrinkage of communication range attributed to environmental effects such as fog, rainfall [13] and temperature [12] [14]. Bannister et al. [12] have shown that the loss of signal strength of telosclass motes takes place with a maximum loss of 8 dB at $65°C$. They have also empirically presented that communication range reduction due to heat is up to 60%. In [14], Boano et al.

have considered deployment of a sensor network in an oil refinery in Portugal. They demonstrated that up to 16% energy can be saved during night and cold season, than other times of the year, due to the mitigation of path loss by the cost of extra transmission and reception energy of the sensor nodes. Nadeem et al. [13], considered the attenuating effects on radio communication due to the rain. They presented relationship between rainfall and attenuating effects on RF communication. WSNs deployed in an area having extreme environmental conditions will affect the performance of sensor nodes and lead to dumb behavior.

B. Characteristics

As mentioned earlier, dumb behavior arises as the transmitting unit of sensor nodes are affected due to environmental phenomena. We have considered two types of nodes in the network – (a) *normal behaved node*, and (b) *dumb node*. In this work, all the sensor node types are considered to be homogeneous, i.e., every node has the same capabilities of sensing, transmitting, and receiving. Let R be the maximum specified communication range of each sensor node. At any instant of time t, let $r_c(t)$ be the communication range of a sensor node. So, $r_c(t) \leq R$. Table I lists all the notations used in this work.

In Figure 1 let R represent the maximum specified fixed communication range of each sensor node, and d_{min} the distance from the node A to its nearest neighbor node.

$$d_{min} = min(r_c^{ne}) \quad \forall ne \tag{1}$$

where, ne is neighbor node, and r_c^{ne} is the communication range of a node when it shrink up to neighbor node ne

Let, at time t_i, the communication range be $r_c(t_i)$. For proper connectivity in the network, each node should maintain the property, $R \geq r_c(t_i) \geq d_{min}$. Due to environmental effects, at time t_j, a node becomes isolated when its communication range shrinks to less than d_{min}, i.e., $r_c(t_j) < d_{min}$.

Attacks versus Dumb behavior: A sensor network is vulnerable to various types of possible attacks such as modification of packets in the network, forceful deactivation of nodes, spreading of wrong information in the network, and jamming [32]. An external user may spread some unnecessary information in the network, and the network can get congested due to which sensor nodes may be unable to transmit their sensed information [33]. An attack differs from dumb behavior. In an attack, the external attacker behaves as “rival” of transmission [34]. In dumb behavior, it is the shrinkage in the communication range due to environmental effects that prevents the transmission of sensed information to the other sensor nodes.

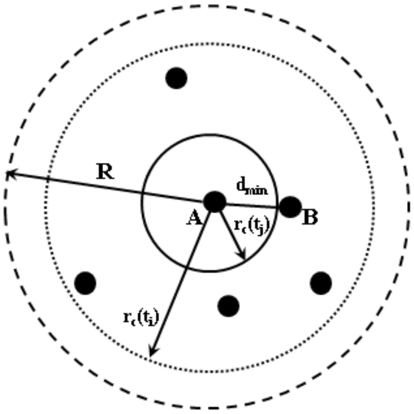


Fig. 1: Shrinkage in Communication Range of a Sensor Node

Intentional deactivation versus Dumb behavior: WSNs are energy-constrained. So, there is always an intention to preserve energy to the maximum possible extent. Certain algorithms may be employed to turn off the transmitting unit to save energy. In case of dumb behavior, the transmitting unit of a sensor node cannot perform its desired functionality, which is unintentional. In intentional deactivation of a sensor node, the node switches off its transmitting unit when it does not need to transmit any data. However, in case of dumb behavior, there may be a situation when a node needs to transmit information, but cannot do so due to shrinkage of communication range of the sensor nodes. So, dumb behavior is completely unintentional and unwanted.

Selfish behavior versus Dumb behavior: In WSNs, a node becomes selfish for conserving its own resources, during which it does not forward other's data, but transmits its own sensed data. The transmission cost in terms of power is more than the other activities in WSNs. Thus, a selfish node can save its power by dropping the packets received from the other nodes. In case of dumb behavior, a node is able to neither send, nor receive any packet due to shrinkage of communication range by the effects of the environment. Though it consumes power, it does not provide any service to the network.

Dead node versus Dumb node: A dead node can neither transmit, nor sense data, as both of its sensing and transmitting units are deactivated due to some disaster, or depletion of energy. These dead nodes stop working permanently. So, they cannot be considered any more for sensing or transmitting any data in the network. Therefore, any protocol designed for use in these networks should have the intention to avoid those nodes for the remaining lifetime of the network. It may be observed that dumb behavior is dynamic in nature, wherein a node starts behaving normally in the absence of environmental effects.

Low energy node versus Dumb node: A sensor node requires more energy for data transmission than sensing. Such a node needs to have an energy level above the threshold for transmission of packets. During the course of operation of the sensor node, its energy reduces and gradually starts dipping below the threshold due to which it can no longer transmit – this node is considered as a low energy node. In case of dumb node, although there may be sufficient energy in the node to sense and transmit, it can sense, but cannot transmit, due to shrinkage in communication range owing to environmental effects. Therefore, a dumb node may convert to a low-energy node during its course of operation when its energy level dips below the threshold.

Definition 1 *Normal Behavior*: A sensor node which can sense physical phenomena in its surroundings and transmit the sensed data during its entire lifetime is termed as normal behaved node. Such behavior is denoted by Ψ_n. Mathematically,

$$\Psi_n = \begin{cases} 1, & (0 < d_{min} \leq r_c(t_i) \leq R) \quad \forall t_i \\ 0, & otherwise \end{cases}$$

Definition 2 *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 different instant of time with the resumption of favorable environmental condition, is termed as a dumb node. Such behavior is denoted by Ψ_d. Mathematically,

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

The state transition diagram of a dumb node is shown in Figure 2. In energy-efficient WSNs, there generally exist two modes of operation – sleep and active. Further, the active state can be split into four states – idle, sense, receive, and transmit. Apart from these states, another state may arise when a sensor node can sense, but not communicate with its neighbors. This state is named as the dumb state.

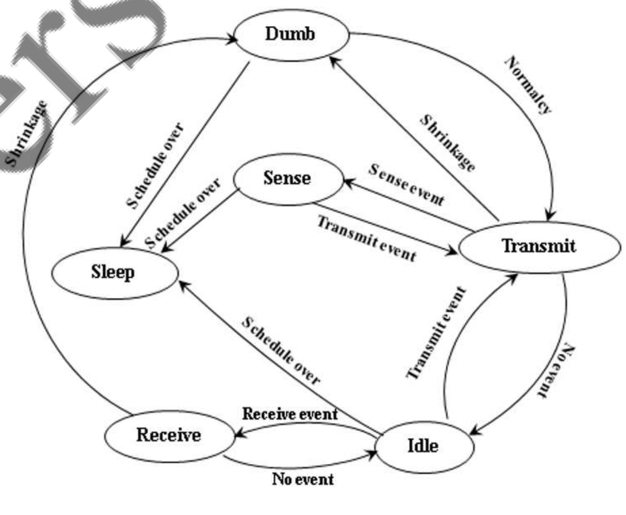


Fig. 2: State Transition Diagram of Dumb Node

Theorem 1. *The probability of dumb behavior of a node increases with the decrease of density in an uniformly* *random deployment of sensor network.*

Proof. Let there be an area, A, where, N number of nodes are deployed.
Node density, $D_N = \frac{N}{A}$.
Probability that a node behaves as dumb is P_{dumb}

$$P_{dumb} = \frac{\pi(d_{min} - \epsilon)^2}{\pi r_c^2} \tag{2}$$

where, ϵ is the shrinkage in communication range from d_{min} and r_c is the communication range

$$P_{dumb} = \frac{(d_{min} - \epsilon)^2}{r_c^2} \tag{3}$$

The number of nodes, N_{disk}, in the unit disk area formed with the communication radius r_c is:

$$N_{disk} = \frac{N}{A}\pi r_c^2 \tag{4}$$

The sensor nodes are uniformly distributed within area A. With the decrease in the number of nodes N in area A, the number of nodes within unit disk area N_{disk} also decreases, in accordance with Equation 4. When the number of nodes N reduces in an area, and they are uniformly distributed, the distance between the nodes also increases, thereby leading to increase in d_{min}. From Equation 3, the probability of a node being dumb P_{dumb} also increases with the increase of d_{min}. Hence, the decrease in density of nodes also increases the probability of a node being dumb. □

V. Effect of the Existence of Dumb Nodes in WSNs

Initially, it is assumed that sufficient number of sensor nodes are deployed in an area. Among the deployed nodes, few nodes are activated to cover the entire area, and the remaining ones are in the sleep mode [35]. In Figure 3, both the active and sleep nodes are shown. A sensor node can communicate with the sink through single-hop or multi-hop communication. In multi-hop communication, the intermediate nodes forward packets to the upstream node. Different environmental effects such as fog, rainfall, and temperature causes increased noise, fading, and, attenuation in the communication channel, reduces the Received Signal Strength (RSS) at the receiver end. In communication, there exists a threshold, RSS_{th}, of RSS above which a node receives data successfully, and processes those data. As signal strength reduces due to environmental effects, a node fails to communicate with its nearest neighbor node, which leads a sensor node to exhibit dumb behavior. The existence of dumb nodes degrades the network operations in different respects, as described in Subsections V-A to V-D.

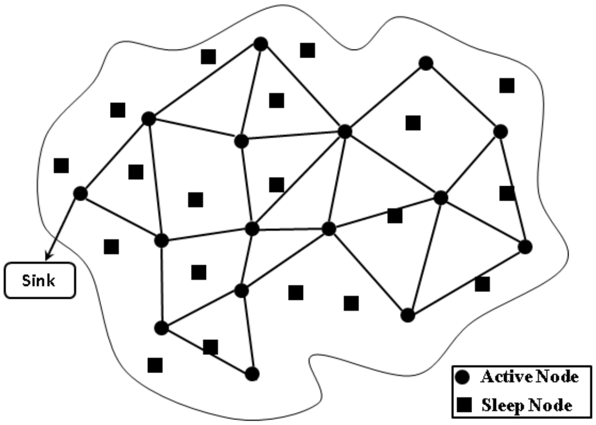
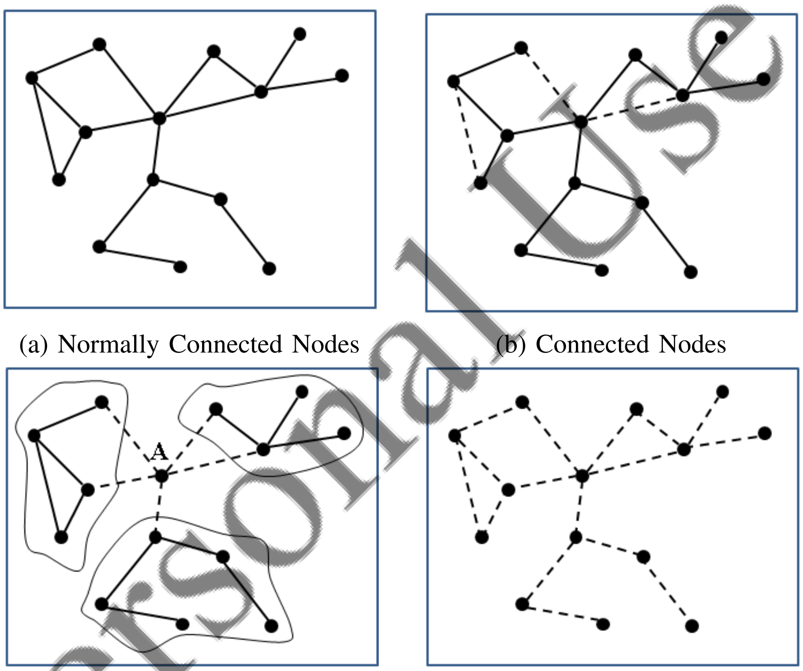


Fig. 3: Normal Wireless Sensor Networks



(a) Normally Connected Nodes

(b) Connected Nodes

(c) Disconnected Group of Nodes

(d) Fully Disconnected Nodes

Fig. 4: Change in Topology due to Shrinkage of Communication Range

A. Connectivity

Connectivity is an important issue in a sensor network for sending sensed information to the sink. An increased number of dumb nodes in a network leads to increased loss in connectivity between its nodes. Depending upon the intensity of the environmental effects, the shrinkage in communication range of a node varies, thereby resulting in split of network, shrinkage of network, and isolation of the nodes. Few possible types of topologies attributed to connectivity loss are shown in Figure 4.

Figure 4a shows a network in normal condition, i.e., there is no environmental effect on it. In Figure 4b, the intensity of the environmental effect is very low. Therefore, although the RSS is reduced, entire connectivity between the nodes is not lost. The connectivity is indicated by dotted line. Figure 4c shows that node A is affected by environment effects, and the network gets split.In Figure 4d, it is shown that due to high intensity of the environmental effects, all the nodes in the network get isolated.

The presence of dumb nodes causes loss of connectivity in the network, as a result of which communication holes may develop. For reconnecting the isolated nodes, or split networks, it is required to activate some of the intermediate sleep nodes. For prolonging the network lifetime, we should have intention to activate a set of intermediate sleep nodes to re-establish connection between the disconnected ones. The dumb behavior is inherently dynamic. So, with the removal of environmental effects, a dumb node starts behaving normally. Therefore, the newly activated nodes need to be deactivated with the onset of favorable environmental conditions.

Theorem 2. *Power consumption for re-construction of lost connectivity increases with the increase in intensity of adverse environmental effects.*

Proof. Let the intensity of environmental effect E_i, and shrinkage in communication range increase (decrease) with the increase (decrease) of E_i. Let the communication range and distance between two nodes A and B be r_c and d, respectively. A minimum number of nodes N_{min} need to be activated between these two nodes A and B for establishing connection, if and only if each activated node lies on the straight line (d) connecting these two nodes, and on the circumference of one another, as shown in Figure 5. Here, nodes A and B are disconnected, and the communication radius of these nodes is r_c. To establish connectivity between these two nodes, nodes 1, 2, and 3 are required to be activated.

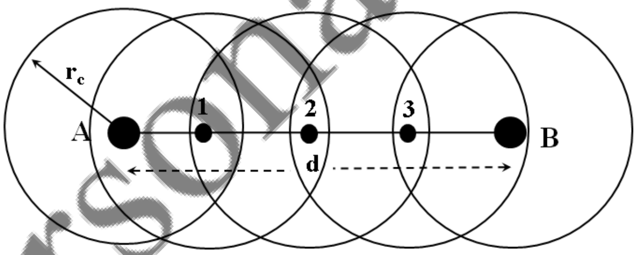


Fig. 5: Minimum Nodes Required To Activated Between Two Nodes

$$N_{min} = \left\lceil \frac{d}{R} \right\rceil - 1 \tag{5}$$

For environmental effect at time t_i, the communication range is reduced by $\Delta r_c(t_i)$. Thus, the communication range will be $r_c - \Delta r_c(t_i)$. Minimum number of nodes require to activate to re-establish connection between node A and B at time instant t_i is:

$$N_{min}(t_i) = \left\lceil \frac{d}{r_c - \Delta r_c(t_i)} \right\rceil - 1 \tag{6}$$

Let the power consumption to activate each node be P. Then, to activate $N_{min}(t_i)$ number of nodes, $P_T(t_i) = P \times N_{min}(t_i)$. At time instant t_j, due to increased intensity of the environmental effect, let the decrease in communication range be $\Delta r_c(t_j)$, such that $\Delta r_c(t_j) > \Delta r_c(t_i)$. The reduced communication radius of each node is $r_c - \Delta r_c(t_j)$, and the minimum number of nodes $N_{min}(t_j)$ required to be activated between two nodes for re-establishment of connectivity:

$$N_{min}(t_j) = \left\lceil \frac{d}{r_c - \Delta r_c(t_j)} \right\rceil - 1 \tag{7}$$

The power consumption to activate these nodes is:

$$P_T(t_j) = P \times N_{min}(t_j) \tag{8}$$

From Equations 6 and 7, $N_{min}(t_j) > N_{min}(t_i)$, as $\Delta r_c(t_j) > \Delta r_c(t_i)$. Thus,

$$P_T(t_j) > P_T(t_i) \tag{9}$$

Hence, it is proved that power consumption for the re-construction of lost connectivity is dependent on the intensity of environmental effect. □

B. Routing

WSNs are multi-hop communication networks, in which every node can sense as well as forward data packets to other nodes. As dumb node can sense but cannot communicate with its neighbors, and is unable to route data packets to the other node(s). A node sending data packets to the other nodes through some intermediate node may start exhibiting dumb behavior among these intermediate node(s). In order to avoid dumb node(s), the sender node may choose another path to route data packets. It may happen that the newly chosen path for routing is longer than the previous one. As the dumb behavior of a sensor node is dynamic in nature, the routing decision should also be taken dynamically.

C. Power Consumption

A node, while exhibiting dumb behavior, unnecessarily remains activated and consumes energy without providing any significant functionality to the network. Dumb nodes in the network create holes, and need to be covered by activating other sleeping neighboring nodes of the dumb one. In this situation, power is consumed by both the dumb and the newly activated neighboring nodes. Hence, due to the presence of dumb nodes, the overall energy consumption of the network increases, and accordingly, the lifetime of the network decreases.

D. Throughput

In a multi-hop sensor network, a source node sends data packets to the sink nodes through one or more intermediate nodes. If one or more intermediate nodes start behaving dumb, the packets that are already sent by the source node, but have not reached the destination will be lost, and the source node has to retransmit those packets to the destination through a different path. This introduces delay in packet transmission, i.e., less number of packets are received by the destination node per unit time. Hence, the throughput of the network degrades. This, in turn, affects the performance of the network by varying routing decisions, which can increase the overhead on the network operation and delay in packet delivery by taking longer path.

Theorem 3. *The transmission delay from a source node to a destination node increases with the increase in hop count from the dumb node to the source node.*

Proof. Let there be I_N number of nodes on the path between the source and the destination nodes. Therefore, $L_C^{I_N} = I_N + 1$ number of links are present on the path between the source and the destination. Time taken by a node needs to transmit a data packet to its immediate neighbor node is t_i

Then, successful transmission time $T_{success}$ to reach a packet from a source node to a destination node is given by:

$$T_{success} = \sum_{i=1}^{I_N+1} [t_i] \tag{10}$$

Let the d^{th} node among the I_N such nodes between the source and destination nodes exhibit dumb behavior. If the d^{th} node shows dumb behavior, then the packet reaches up to the $(d-1)^{th}$ and informs the source node that the d^{th} node is dumb. Time for unsuccessful packet delivery is:

$$T_{unsuccess} = \sum_{i=1}^{k}[t_i] + \sum_{j=d-1}^{1} [t_j] \tag{11}$$

where, $\sum_{i=1}^{k}[t_i]$ is the transmission time up to the d^{th} node, and $\sum_{i=1}^{k}[t_i]$ is the error propagation time from the $(d-1)^{th}$ node to the source node. In a reliable WSN, if a packet is not delivered to destination, it needs to re-transmit, as mentioned in [36]–[39]. A packet, which is not delivered due to the presence of dumb node, needs to be re-transmitted, and for re-transmission it is required to have normal transmission time. When the source node is knowledgable about the existence of a dumb node in the path, it needs to establish the path again. Let this time be

T_{path}. The time needed for re-transmission, $T_{retransmit}$, is given by:

$$T_{retransmit} = \sum_{k=1}^{{I_N}^{'}} [t_k] \tag{12}$$

where ${I_N}^{'}$ is the number of intermediate nodes in the new path and $I_N \neq {I_N}^{'}$. Again the total time T for packet transmission when d^{th} node behaves as dumb is given by:

$$T = T_{unsuccess} + T_{path} + T_{retransmit} \tag{13}$$

$$T = \sum_{i=1}^{k} [t_i] + \sum_{j=d-1}^{1} [t_j] + T_{path} + \sum_{k=1}^{{I_N}^{'}} [t_k] \tag{14}$$

With the increase in $d's$ value (hop count from source to destination), T also increases.

Hence, the transmission delay will increases with the increase in hop count from the dumb node to the source node. □

Algorithm 1 Dumb behavior in WSN

Require:

- N_{total}: Total number of nodes
- N_{dumb}: Number of dumb nodes
- T_{sim}: Network operation time
- xlen: width of terrain along x-axis
- ylen: width of terrain along y-axis
- τ_{normal}: Maximum time duration for normal behavior
- τ_{dumb}: Maximum time duration for dumb behavior
- r_c: Communication range of nodes

```
SinkNode ← Node [0]
SourceNode ← Node [$N_{total}$ - 1]
Select $N_{dumb}$ nodes form $N_{total}$ nodes
while $t \leq T_{sim}$ do                                  ▷ t is the current time
    $t_{dumb}$ ← Random time duration in [1, $\tau_{dumb}$]
    while $t_{dumb} \geq 0$ do
        Choose a communication range between 0 and $r_c$
        Stop $T_X$ and $R_X$ of selected $N_{dumb}$ nodes
        $t_{dumb}$ = $t_{dumb}$ - 1
    end while
    $t_{normal}$ ← Random time duration in [1, $\tau_{normal}$]
    while $t_{normal} \geq 0$ do
        Choose a communication range between $r_c$
        Start $T_X$ and $R_X$ of selected $N_{dumb}$ nodes
        $t_{normal}$ = $t_{normal}$ - 1
    end while
    t = t + 1
end while
```

VI. Simulation Design And Results

A. Simulation Design

Algorithm 1 is capable of inducing dumb behavior on some of the nodes in a sensor network, where all nodes behave normally. These nodes exhibit both dumb behavior and normal behavior periodically for random duration of time. For simulating the scenario and analyzing the effect of dumb nodes on the performance of WSNs, we used the NS-3 simulator. We deployed 40-100 sensor nodes, including a sink node, randomly over a 250 m × 250 m simulation area. We considered the effects on different performance parameters of the network by varying the number of dumb nodes from 10-50%, in an interval of 10%. In plots, we have shown the effects on performance metrics of a WSN in the presence of dumb, selfish, and dead sensor nodes. In each of these plots, it is observed that performance degrades in the presence of a dumb nodes, compared to the normal scenario, i.e., when all nodes are normally behaved. The list of simulation parameters is shown in Table II.

TABLE II: Simulation Parameters

Parameter	**Value**
Number of nodes	40-100
Number of dumb nodes	10-50
Simulation area	250m × 250m
Number of data packets	100
Packets Length	512 bytes
Routing Protocol	AODV, OLSR, GPSR
Packet Interval	10 Sec
Communication range	40-60 m
Initial Energy	0.75J

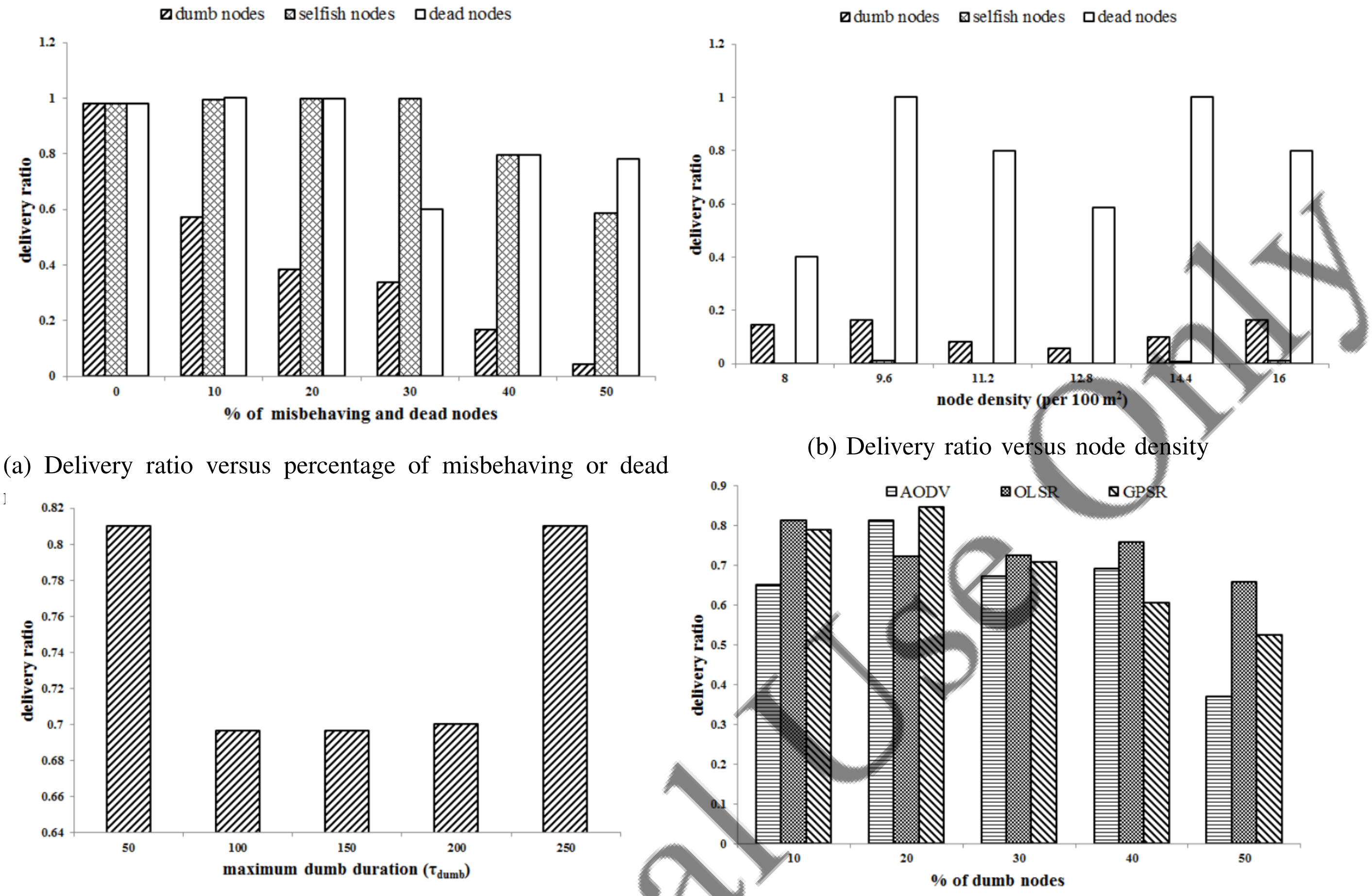
In the experiments, we have considered the nodes to be stationary in the simulated networks. We considered that 100 packets are sent with a packet interval of 10 seconds. We have compared the effect of dumb nodes using the well-known reactive routing protocol, AODV [40], proactive routing protocol, OLSR [41], and position-based stateless routing protocol, GPSR [42], similar to another stateless protocol SPEED [43]. The scenario is simulated over T_{sim} = 1000 seconds of simulation time. The time for dumb behavior of a node is taken as t_{dumb} and the time for normal behavior of a node is taken as t_{normal}. Both t_{dumb} and t_{normal} are chosen randomly in the range 1 to τ_{dumb} and 1 to τ_{normal}. For simplicity, we have taken both τ_{dumb} and τ_{normal} to be equal and varying between 50 and 250 seconds of simulation time. For simulating the environmental effect on sensor nodes, the communication range of these nodes were randomly varied between 40-60 m. We simulated three types of node behavior – *dumb, selfish*, and *dead*. We also compared between these node behaviors with respect to different network parameters– throughput, average end-to-end delay, delivery ratio, energy, and network lifetime.

B. Results Of Performance Evaluation

The result of simulation were plotted on different graphs to represent the effect of dumb, selfish, and dead nodes on a sensor network. Figure 6a shows the effect of these on the delivery ratio of data packets in WSNs. Here, we observe how the presence of these three types of nodes in the networks creates detrimental effects on the delivery ratio. The delivery ratio is calculated as N'/N, where N' is the number of packets received, and N is the total number of packets sent. A source node sends some data packets to the sink over single-hop or multi-hop communication links. Due to these node behaviors, some data packets may be lost and cannot reach the destination. Few of the data packets reach the sink. Therefore, in normal scenario, the delivery ratio of the network will be close to unity. However, in the presence of these misbehaving or dead nodes, delivery ratio is less than unity. Figure 6b shows the effect on delivery ratio in the networks due to the presence of these nodes with varying node density. Figure 6c shows the change in delivery ratio in presence of dumb node, with varying maximum dumb duration (τ_{dumb}). Effect on delivery ratio with varying percentage of dumb nodes using different routing protocols is shown in Figure 6d.

Figure 7 shows the average end-to-end delay of transmitted data packets from source to sink. Figure 7a plots the delay in the presence of dumb, selfish, and dead nodes in WSN with varying percentage of these nodes. A source node sends data packets to sink over single-hop or multi-hop communication while incorporating delay in packet transmission. Different data packets may follow different paths to reach the destination. Therefore, these different packets take different times to reach the destination. In this work, we considered the average time for packet sending from source to sink. It shows that the average delay in the presence of misbehaving or dead nodes is more than having all normal behaved nodes in the network. Figure 7b represents the average delay in the presence of misbehaving and dead nodes in WSN with varying node density in the network. The variation of end-to-end delay for packet delivery in the presence of dumb node, with the change in the maximum dumb duration (τ_{dumb}) is plotted in Figure 7c. The effect on average end-to-end delay with different percentage of dumb nodes using different routing protocol is shown in Figure 7d.

Throughput is also affected in the presence of dumb nodes in the network. Figure 8 shows the detrimental effects of the presence of dumb nodes on the throughput of WSNs. Throughput is calculated using the formula N×S$\sum_{i=1}^{n}(1/t_i)$, where N is the number of packets received, S is the packet size and t_i is the end-to-end delay for the i^{th} packet. It is observed that throughput is less in the network in the presence of dumb nodes compared to the case in which all nodes in the network are normal behaved. Figures 8a and 8b show the variation in throughput with different percentages of dumb, selfish, dead nodes, and with different node densities. The variation of network throughput in the presence of dumb node, with change in maximum dumb duration (τ_{dumb}), is plotted in Figure



(a) Delivery ratio versus percentage of misbehaving or dead

(b) Delivery ratio versus node density

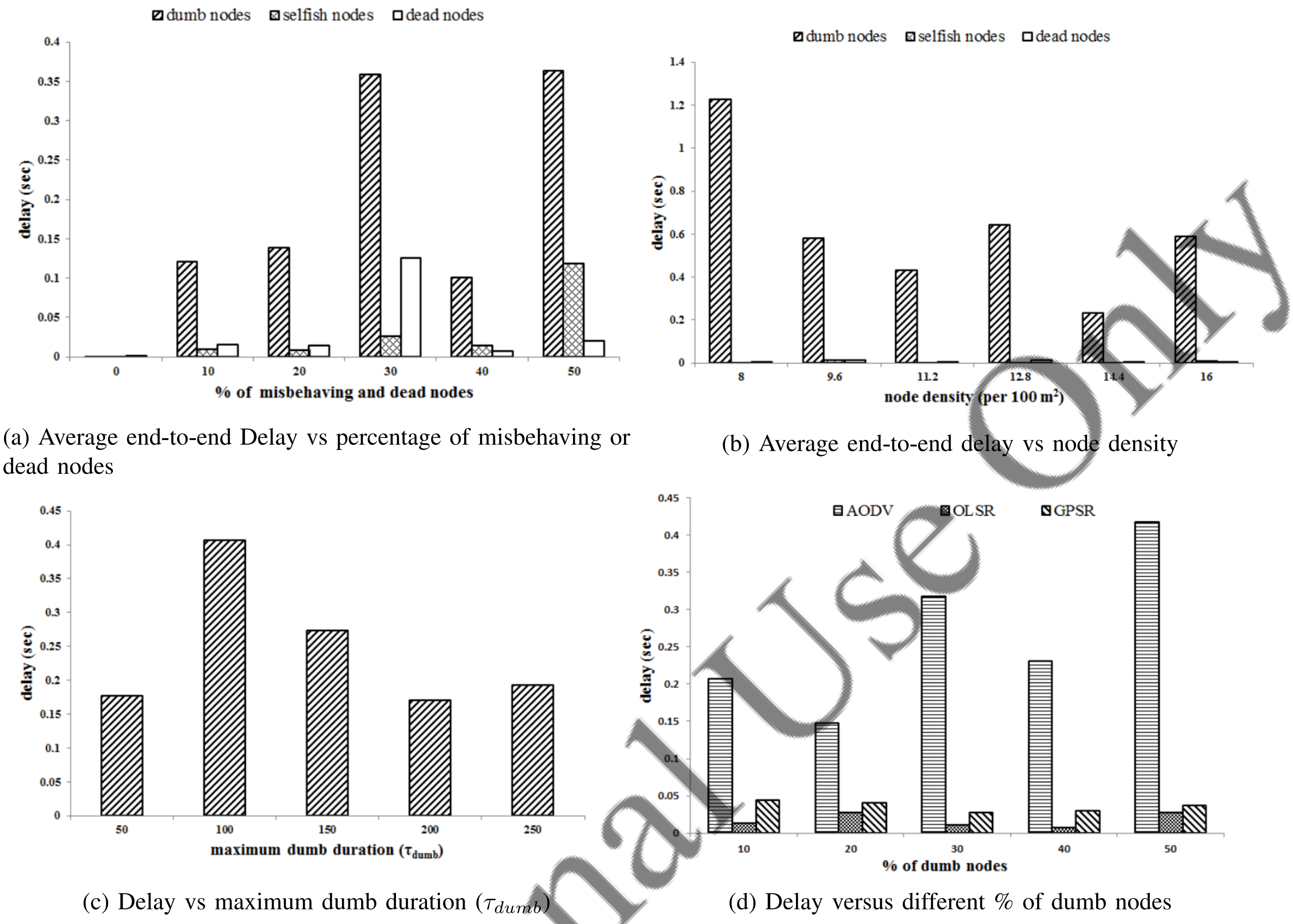
(c) Delivery ratio vs maximum dumb duration (τ_{dumb})

(d) Deliveryratio versus different % of dumb nodes

Fig. 6: Delivery ratio

8c. The throughput of the network in the presence of dumb nodes varies when different routing protocols are used. Figure 8d shows the effect on throughput of the network with different percentage of dumb nodes using different routing protocols.

In Figures 6, 7, and 8, we observe that the network performance degrades in the presence of dumb nodes. The performance of the network does not always degrade with the increasing number of misbehaving or dead nodes. We considered random deployment of nodes and selected dead and misbehaving nodes randomly. When the randomly selected dead or misbehaving nodes are not on the routed path from source to sink, the performance degradation is not significant. On the other hand, if these randomly selected dumb nodes are on the routed path, the performance of the network is seriously affected. Also, the initial node activation schemes for covering the entire region also affects the performance of the network in the presence of dumb nodes. Figures 6d, 7d and 8d illustrate that performance decreases starting from AODV to GPSR to OLSR in terms of delivery ratio, average end-to-end delay and network throughput. The possible reason for such deterioration is because the AODV routing protocol is



(a) Average end-to-end Delay vs percentage of misbehaving or dead nodes

(b) Average end-to-end delay vs node density

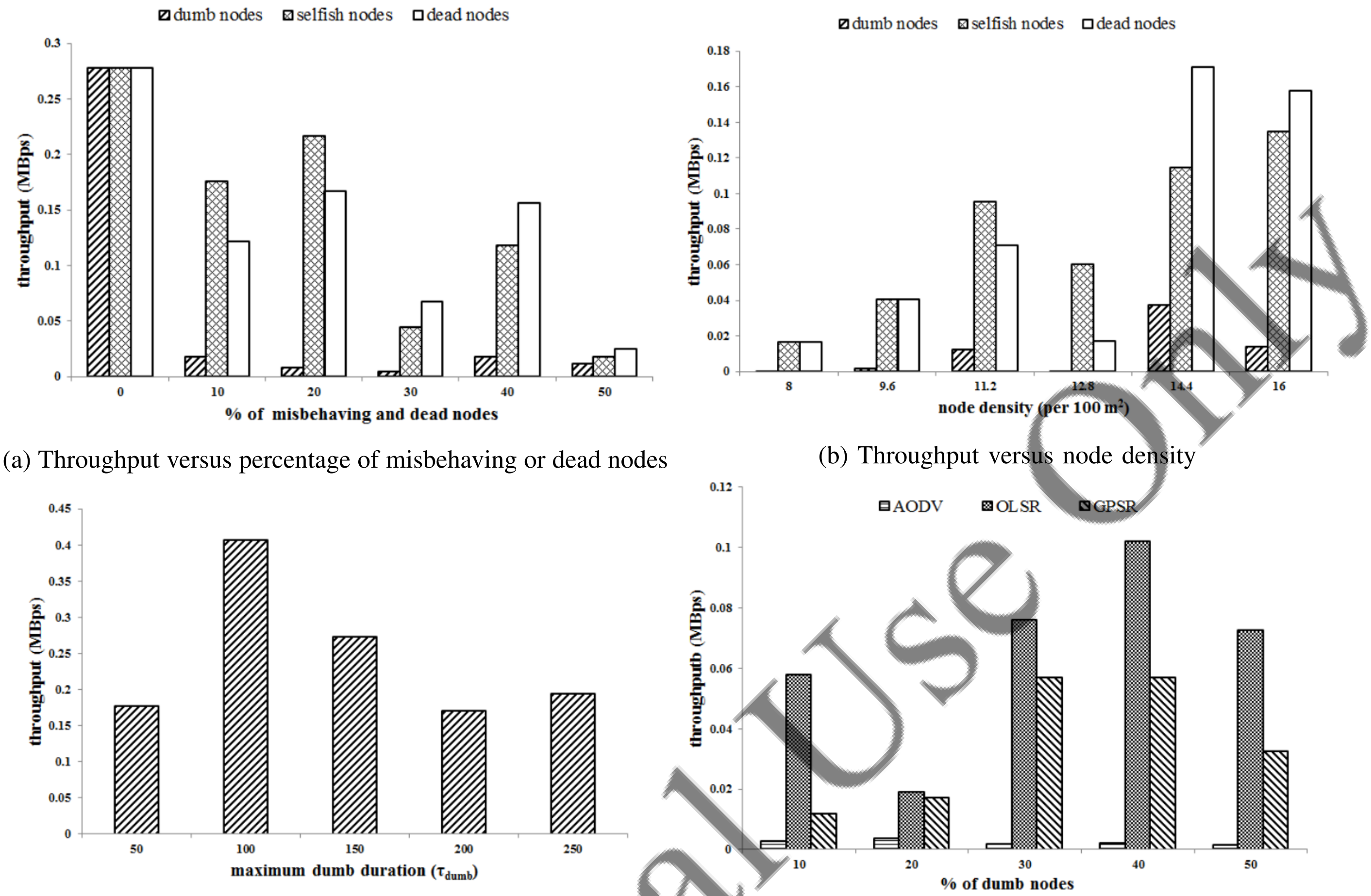
(c) Delay vs maximum dumb duration (τ_{dumb})

(d) Delay versus different % of dumb nodes

Fig. 7: Average end-to-end delay

reactive, whereas OLSR and GPSR are proactive routing protocols. In a static network, the proactive protocol renders better performance than the reactive routing protocol. In our study, we have taken a static network. Consequently, OLSR and GPSR shows better performance than AODV. In OLSR, a source node selects few neighbor nodes as Multipoint Relays (MPRs), so that it can establish connectivity up to two-hop neighbors from itself, which may not be the farthest node from the source node. In GPSR a source node selects a neighbor node as forwarding node which is nearest to the destination node and therefore, farthest from itself. The probability that a forwarding node being outside the reduced communication range is higher in GPSR, compared to probability of MPR nodes in case of OLSR. Therefore, the selection of new path is more frequent in GPSR than in OLSR. Hence, OLSR gives better performance than GPSR.

The sensor nodes consume energy for reception and transmission of data packets. Figures 9a and 9b depict the total energy consumption in the network in the presence of 25% and 50% of misbehaving or dead nodes, respectively.



(a) Throughput versus percentage of misbehaving or dead nodes

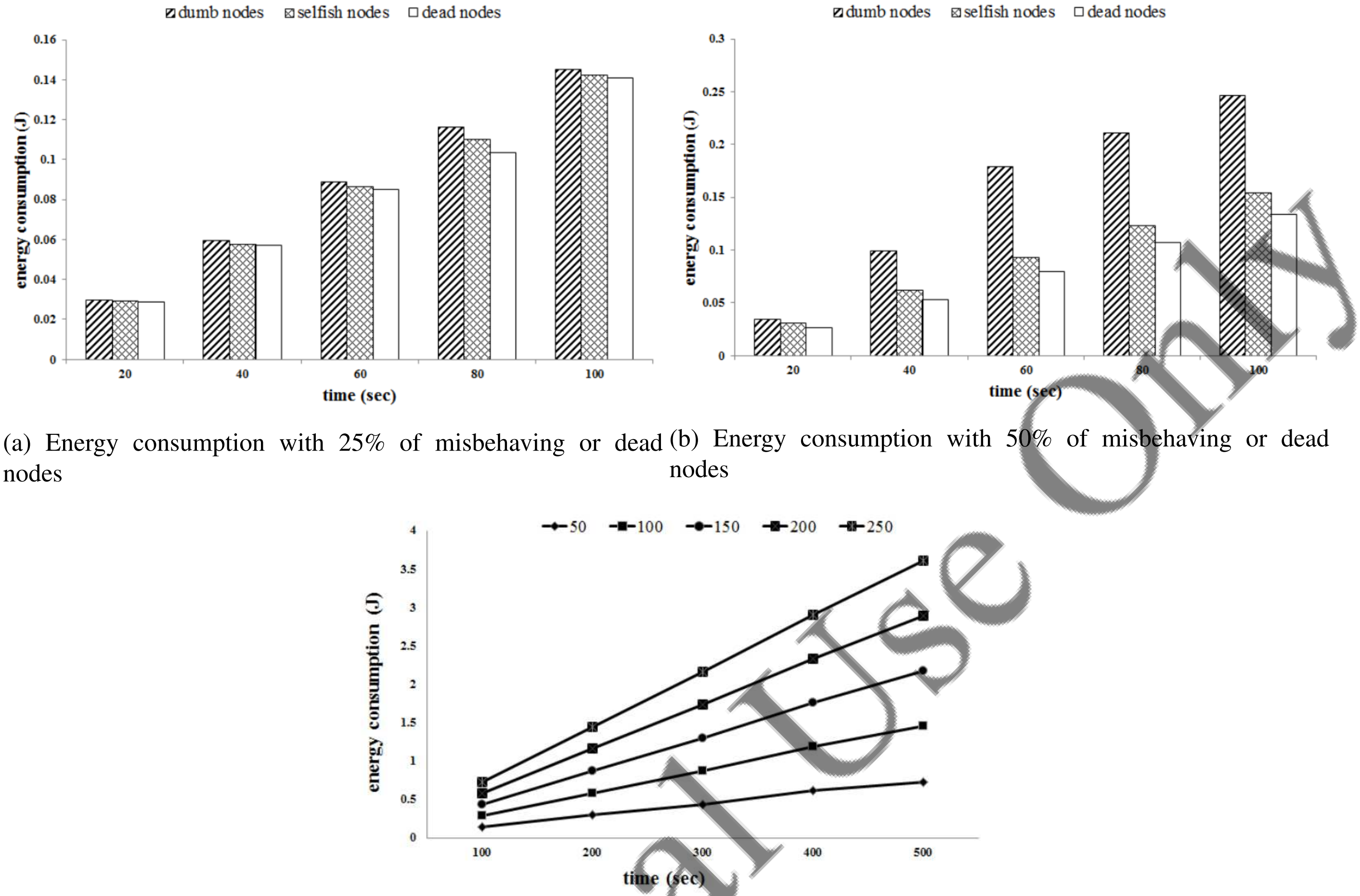
(b) Throughput versus node density

(c) Throughput vs maximum dumb duration (τ_{dumb})

(d) Throughput versus different % of dumb nodes

Fig. 8: Throughput

A gradual increase in the total energy consumption of the network with time is observed. It is noteworthy that the total energy consumption in the presence of dumb nodes is more than that in the presence of selfish nodes, which, in turn, is more than in the case of dead nodes. Due to the shrinkage of communication range, dumb nodes cannot communicate with the other nodes, but their transmission and reception units remain activated. So, dumb nodes consume the same amount of energy as in the normal nodes. Selfish nodes can only transmit to others nodes, but cannot receive from them. So, selfish nodes consume energy only for transmission, and not for reception of data packets. Hence, total energy consumption in the presence of selfish nodes is less that than in the presence of dumb nodes in the network. In case of dead nodes, both the transmission and reception units are non-operational. So, the total energy consumption of the network is the lowest in the presence of dead nodes. Figure 9c shows the energy consumption of the network in the presence of dumb nodes, with varying maximum dumb duration. This figure shows that an increase in the maximum dumb duration increases the energy consumption of the network.

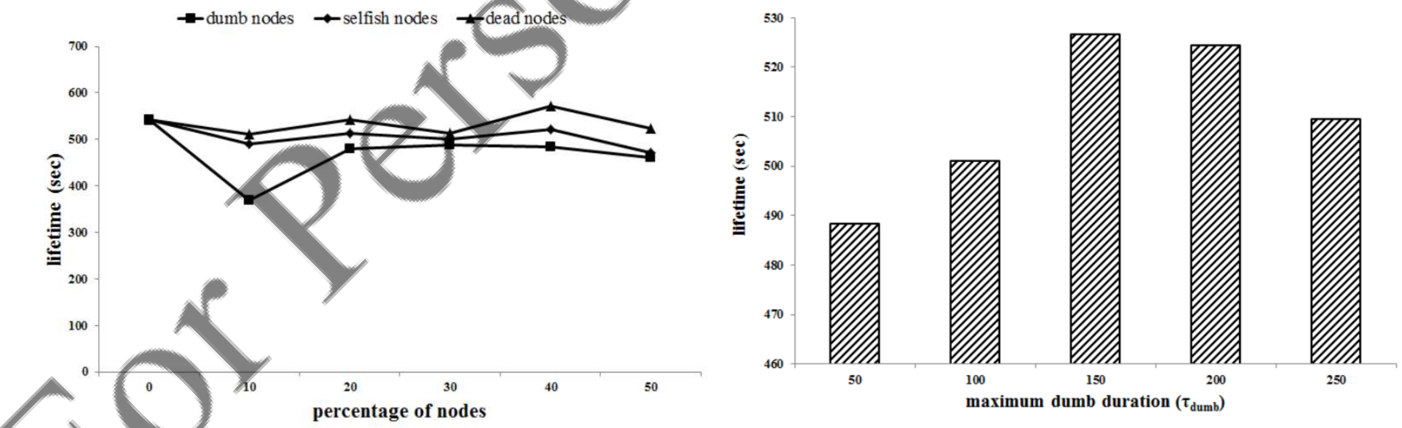


(a) Energy consumption with 25% of misbehaving or dead nodes

(b) Energy consumption with 50% of misbehaving or dead nodes

(c) Energy consumption for different τ_{dumb}

Fig. 9: Energy consumption



(a) Lifetime versus percentage of misbehaving or dead nodes

(b) Lifetime for different τ_{dumb}

Fig. 10: Lifetime

The possible reason is that, when nodes start to behave dumb for more duration of time, other normal behaved nodes also have to participate in communication for more duration of time, which consumes more energy while dumb nodes are also consuming energy without providing services for communication.

Network lifetime is also an important parameter for performance measurement. Network lifetime is the time duration for which the total remaining energy of the network is above zero, i.e., the time duration for which the network remain alive. Figure 10a shows that the lifetime of the network in the presence of dumb nodes is less than that in the presence of selfish nodes, which, in turn, is less than that in the presence of dead nodes in the network. From this Figure, it is observed that the total energy consumption in the presence of dumb nodes is more than that in the presence of selfish nodes, which is also more than that in the presence of dead nodes in the network. Consequently, lifetime of the network in the presence of dumb nodes is less than that in the presence of selfish nodes, which is also less than that in the presence of dead nodes. Figure 10b shows the variation of lifetime of the network with varying maximum dumb duration.

VII. Conclusion

In this work, we have considered an unexplored behavior of the sensor nodes – dumb behavior – which adversely affects the overall performance of WSNs. This type of behavior of sensor nodes is considered as a type of misbehavior due to its similarity of impact with other type of misbehavior in the network. The simulation results indicate the negative impact on network performance and energy consumption of a stationary WSNs in the presence of dumb nodes. To eliminate the effect of dumb nodes on the performance of the WSNs, these nodes should be avoided in the regular network operations.

In the future, we plan to extend our work with respect to dumb node detection in WSNs, dumb probability estimation, network connectivity, and reduction in energy consumption, thereby making routing more energy-efficient. The detection of dumb node is an essential part of topology management in WSN and it can be done using Markov chain analysis of a node's state or by using a mobile agent. Recovery from the effect of dumb nodes can be done by establishing connectivity between the disconnected nodes with the help of the intermediate sleep nodes. A subset of the intermediate sleep nodes should be activated to establish best possible connectivity between two disconnected nodes. Another possible way of exchanging information between two disconnected nodes is using mobile relay node.

References

[1] 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.

[2] F. Zabin, S. Misra, I. Woungang, H. Rashvand, N.-W. Ma, and M. A. Ali, “REEP: A Data-Centric, Energy-Efficient and Reliable Routing Protocol for Wireless Sensor Networks,” *IET Communications*, vol. 2, no. 8, pp. 995–1008, 2008.

[3] S. K. Dhurandher, S. Misra, M. S. Obaidat, V. Bansal, P. Singh, and V. Punia, “EEAODR: An Energy-Efficient On-Demand Routing Protocol for Wireless Ad-Hoc Networks,” *International Journal of Communication Systems*, vol. 22, no. 7, pp. 789–817, 2009.

[4] R. Chandrasekar, S. Misra, and M. S. Obaidat, “A Probabilistic Zonal Approach for Swarm-Inspired Wildfire Detection Using Sensor Networks,” *International Journal of Communication Systems (Wiley)*, vol. 21, no. 10, pp. 1047–1073, 2008.

[5] S. Misra and S. Singh, “Localized policy-based target tracking using wireless sensor networks,” *ACM Transactions on Sensor Networks (TOSN)*, vol. 8, no. 3, August 2012.

[6] S. Misra, B. J. Oommen, S. Yanamandra, and M. S. Obaidat, “Random Early Detection for Congestion Avoidance in Wired Networks: The Discretized Pursuit Learning-Automata-Like Solution,” *IEEE Transactions on Systems, Man and Cybernetics Part B*, vol. 40, no. 1, pp. 66–76, 2010.

[7] S. Misra, V. Tiwari, and M. S. Obaidat, “LACAS: Learning Automata-Based Congestion Avoidance Scheme for Healthcare Wireless Sensor Networks,” *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 466–479, May 2009.

[8] M. Drozda, S. Schaust, and H. Szczerbicka, “AIS For Misbehavior Detection In Wireless Sensor Networks: Performance and Design Principles,” in *Proceedings of IEEE Congress on Evolutionary Computation*, Singapore, 2007, pp. 25–28.

[9] H. Huangshui and Q. Guihe, “Fault Management Frameworks in Wireless Sensor Networks,” in *Proceedings of Intelligent Computation Technology and Automation*, vol. 2, Guangdong, China, March 2011, pp. 1093 –1096.

[10] G. Anastasi, A. Falchi, A. Passarella, M. Conti, and E. Gregori, “Performance Measurements of Motes Sensor Networks,” in 7th *ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2004, pp. 174–181.

[11] L. Paradis and Q. Han, “Dealing with Faults in Wireless Sensor Networks,” *Journal of Network and Systems Management*, vol. 15, pp. 171–190, June 2007.

[12] K. Bannister, G. Giorgetti, and E. K. S. Gupta, “Wireless Sensor Networking For Hot Applications: Effects Of Temperature On Signal Strength, Data Collection and Localization,” in *Proceedings of* 5th *Workshop on Embedded Networked Sensors*, 2008.

[13] F. Nadeem, S. Chessa, E. Leitgeb, and S. Zaman, “The Effects of Weather on the Life Time of Wireless Sensor Networks Using FSO/RF Communication,” *Radio Engineering*, vol. 19, no. 2, pp. 262–270, June 2010.

[14] C. A. Boano, N. Tsiftes, 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.

[15] A. Fanimokun and J.Frolik, “Effects Of Natural Propagation Environments On Wireless Sensor Network Coverage Area,” in *Proceedings of the* 35th *Southeastern Symposium on System Theory*, March 2003, pp. 16–20.

[16] S. Misra, M. P. Kumar, and M. S. Obaidat, “Connectivity Preserving Localized Coverage Algorithm for Area Monitoring Using Wireless Sensor Networks,” *Computer Communications (Elsevier)*, vol. 34, no. 12, pp. 1484–1491, 2011.

[17] J. Bonvoisin, A. Lelah, F. Mathieux, and D. Brissaud, “An Environmental Assessment Method For Wireless Sensor Networks,” *Journal of Cleaner Production*, vol. 33, pp. 145–154, September 2012.

[18] S. K. Dhurandher, S. Misra, M. S. Obaidat, and N. Gupta, “An Ant Colony Optimization Approach for Reputation and Quality-of-Service-Based Security in Wireless Sensor Networks,” *Security and Communication Networks*, vol. 2, no. 2, pp. 215–224, 2009.

[19] S. Misra and A. Jain, “Policy Controlled Self-Configuration in Unattended Wireless Sensor Networks,” *Journal of Networks and Computer Applications*, vol. 34, no. 5, pp. 1530–1544, Sept 2011.

[20] S.-J. Yim and Y.-H. Choi, “Neighbor-Based Malicious Node Detection in Wireless Sensor Networks,” in *Wireless Sensor Network*, vol. 4, no. 9, Sept 2012, pp. 219–225.

[21] L. B. Ruiz, I. G. Siqueira, L. B. e Oliveira, H. C. Wong, J. M. S. Nogueira, and A. A. F. Loureiro, "Fault Management in Event-Driven wireless Sensor Networks," in *Proceedings of the 7^{th} ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2004, pp. 149–156.

[22] R. Kannan, S. Wei, V. Chakravarthi, and G. Seetharaman, "Analysis of Communication Vulnerability through Misbehavior in Wireless and Sensor Networks," in *Proceedings of Military Communications Conference*, October 2005, pp. 1040–1046.

[23] B. Khelifa, A. Bechar Univ., H. Haffaf, M. Madjid, and D. Llewellyn-Jones, "Monitoring Connectivity in Wireless Sensor Networks," in *Proceedings of Symposium on Computers and Communications*, July 2009, pp. 507–512.

[24] X. Liu, "Coverage with connectivity in wireless sensor networks," in *3rd International Conference on Broadband Communications, Networks and Systems*, October 2006, pp. 1–8.

[25] X. H. K. Yin, "The Optimized Deployment Scheme to Maintain Connectivity in Wireless Sensor Networks," in *International Conference on Machine Vision and Human-Machine Interface*, April 2010, pp. 405–408.

[26] C. A. Kamhoua, N. Pissinou, J. Miller, and S. K. Makki, "Mitigating Routing Misbehavior in Multi-hop Networks Using Evolutionary Game Theory," in *GLOBECOM Workshops on Advances in Communications and Networks*, Florida, USA, 2010, pp. 1957–1962.

[27] M. Probst and S. Kasera, "Statistical Trust Establishment In Wireless Sensor Networks," in *Proceedings of International Conference on Parallel and Distributed Systems*, vol. 2, Hsinchu, Taiwan, December 2007, pp. 1–8.

[28] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-demand Secure Routing Protocol Resilient to Byzantine Failures," in *Proceedings of 1^{st} ACM workshop on Wireless security*, 2002.

[29] S. Misra, P. V. Krishna, K. I. Abraham, N. Sasikumar, and S. Fredun, "An Adaptive Learning Routing Protocol for the Prevention of Distributed Denial of Service Attacks in Wireless Mesh Networks," *Computers & Mathematics with Applications (Elsevier)*, vol. 60, no. 2, pp. 294–306, 2010.

[30] D. Z. Tootaghaj, F. Farhat, M.-R. Pakravan, and M.-R. Aref, "Game-theoretic Approach to Mitigate Packet Dropping in Wireless Ad-hoc Networks," in *proceedings of Consumer Communications and Networking*, Nevada. USA, 2011, pp. 63–65.

[31] 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, 2013.

[32] S. Misra, S. K. Dhurandher, A. Rayankula, and D. Agrawal, "Using Honeynodes for Defense Against Jamming Attacks in Wireless Infrastructure-Based Networks," *Computers and Electrical Engineering (Elsevier)*, vol. 36, no. 2, pp. 367–382, 2010.

[33] R. Chandrasekar, S. Misra, and M. S. Obaidat, "FORK: A Novel Two-Pronged Strategy for an Agent-Based Intrusion Detection Scheme in Ad-Hoc Networks," *Computer Communications (Elsevier)*, vol. 31, no. 16, pp. 3855–3869, 2008.

[34] S. Misra, K. I. Abraham, M. S. Obaidat, and P. V. Krishna, "LAID: A Learning Automata-Based Scheme for Intrusion Detection in Wireless Sensor Networks," *Security and Communication Networks (Wiley)*, vol. 2, no. 2, pp. 105–115, 2009.

[35] M. Cardei and D. Du, "Improving Wireless Sensor Network Lifetime through Power Aware Organization," *Wireless Networks (Springer)*, vol. 11, no. 3, pp. 333–340, May 2005.

[36] Y. Iyer, S. Gandham, and S. Venkatesan, "STCP: a generic transport layer protocol for wireless sensor networks," in *Proceedings of Conference on Computer Communications and Networks*, Oct 2005, pp. 449–454.

[37] H. Zhanga, A. Arorab, Y. Choic, and M. G. Goudac, "Reliable bursty convergecast in wireless sensor networks," *Computer Communications(Elsevier)*, vol. 30, no. 13, pp. 2560–2576, Sept 2007.

[38] H. Zhou, X. Guan, and C. Wu, "Reliable Transport with Memory Consideration in Wireless Sensor Networks," in *Proceedings of IEEE International Conference on Communications*, May 2008, pp. 2819–2824.

[39] S. J. Park, R. Vedantham, R. Sivakumar, and I. F.Akyildiz, "A Scalable Approach for Reliable Downstream Data Delivery in Wireless

Sensor Networks," in *Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing*, May 2004, pp. 78–89.

[40] I. D. Chakeres and E. M. Belding-Royer, "AODV Routing Protocol Implementation Design," in *In proceedings of 24th International Conference on Distributed Computing Systems Workshops(ICDCSW'04)*, vol. 7. DC, USA: IEEE Computer Society, Washington, 2004, pp. 698–703.

[41] T. Clausen and P. Jacque, "Optimized link state routing protocol(olsr)," *IETF Request for Comments: 3626*, October 2003.

[42] B. Karp and H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," in *In proceedings of 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom' 02)*, New York, NY, USA, 2000, pp. 243 – 254.

[43] T. He, J. A. Stankovic, C. Lu, and T. Abdelzaher, "SPEED: A Stateless Protocol for Real-Time Communication in Sensor Networks," in *In proceedings of 23rd International Conference on Distributed Computing Systems*, May 2003, pp. 46–55.