# Dectect the Selfishness of Node in Wireless Sensor Network

**Ashutosh Gaur#1, Brajesh Kumar*2, Dr. Pragati Upadhyay*3**

*#1Assistant Professor, Department of Computer Science& Engineering Pranveer Singh Institute of Technology Kanpur U.P (India)*

**2Assistant Professor, Department of Computer Applications Pranveer Singh Institute of Technology Kanpur U.P (India)*

**3Associate Professor, Department of Computer Applications PSIT College of Higher Education Kanpur U.P (India)*

***Abstract: -*** This study examines the self-centered conduct of nodes in Wireless Sensor Networks (WSN). Uncooperative node behavior, termed selfishness, involves nodes attempting to exploit others while refusing to relay their packets. The research addresses all forms of selfishness, aiming to identify and isolate selfish nodes from data packet forwarding. Various strategies to combat selfishness have been proposed in existing literature. However, most approaches focus on detecting and preventing individual node misconduct, leaving them susceptible to coordinated attacks by multiple adversaries. The importance of addressing selfish behavior in WSN using bonus-based methods lies in maximizing network throughput. This objective can be achieved through the application of game theory principles.

***Keywords****:* wireless sensor network (WSN), Game theory (GT), The Prisoners' Dilemma Problem Scenario

## 1. Introduction

A **wireless sensor network (WSN)** is composed of autonomous sensors distributed across an area to monitor various physical or environmental factors, such as temperatures, sound, and pressure. These sensors work together to transmit their collected data through the network to a central location. Modern WSNs feature two-way communication, allowing for the management of sensor operations. Initially developed for military purposes like battlefield surveillance, WSNs now find applications in numerous industrial and consumer sectors. These include monitoring and controlling industrial processes, assessing machine health, and other emerging uses.

A Wireless Sensor Network (WSN) is composed of numerous sensor nodes that collaboratively monitor a particular area of interest. Typically, a sensor node is a compact device incorporating sensing, power, communication and processing units for data processing, transmission and collection. These nodes aggregate and transmit sensed data to a specialized node called a base station, which serves as an intermediary between sensor nodes and users. The distinctive feature of a sensor node is its compact size and lightweight nature. However, these nodes face various limitations, including restricted resources in terms of energy, memory, processing speed, and bandwidth. As sensor nodes are generally battery-operated, efficient energy management is crucial. Another key concern is maximizing the network's lifespan while monitoring specific targets using randomly distributed sensor nodes. The price of sensor nodes varies significantly, ranging from a few dollars to hundreds, depending on their complexity. The size and cost constraints of sensor nodes lead to corresponding limitations in resources such as energy, memory, computational capacity, and communication bandwidth. WSN topologies can range from basic star networks to sophisticated multi-hop wireless mesh networks. Data propagation between network hops can occur through routing or flooding techniques. We examine the stability and efficiency of wireless networks containing one or more selfish users. "Selfish" users are those willing to manipulate their wireless interface to increase their share of the shared transmission resource; we consider these users to be rational rather than malicious (they are willing to harm others only if they can benefit from such behavior).

## 2. Related Work

The watchdog technique identifies malfunctioning nodes by monitoring their behavior. Consider a network path from S to P via nodes M, N, and O. Although M cannot directly communicate with O, it can observe N's transmissions. When M sends a packet through N to O, M can typically verify if N forwards it. Unless each link is separately encrypted, which is costly, M can also detect if N has modified the payload or header. This method assesses packet throughput, routing overhead percentage, and accuracy in detecting misbehaving nodes. In a moderately mobile network with 40% misbehaving nodes, combining watchdog and path rater increases overhead transmissions from 9% to 17%. In highly mobile conditions, these techniques can boost network throughput by 27%, while increasing overhead from 12% to 24%.

Game theory (GT) is a mathematical approach that analyzes conflict and cooperation among rational decision-makers. GT applications in wireless sensor networks include routing protocol design, topology and power control, energy conservation, packet forwarding, data collection, spectrum and bandwidth allocation, quality of service management, coverage optimization, security, and other network management tasks[2].

Packet dropping by misbehaving nodes significantly degrades ad-hoc network performance. A proposed algorithm surpasses previous methods by resisting collusion attacks and functioning in networks with directional antennas. Additionally, a game-theoretic strategy called ERTFT [3] is introduced to address node behavior.

The current watchdog mechanism's limitations include evaluating only next-hop behavior and broadcasting results, which is neither attack-resistant nor energy-efficient. An enhanced watchdog mechanism is suggested, which monitors all neighboring nodes' behavior based on MAC layer information, in addition to the next-hop [4].

## 3. Work Plan

Game Theory Overview

.GT's functions encompass various aspects of network management, including the development of routing protocols, control of topology and power, energy conservation, forwarding of packets, gathering of data, allocation of spectrum and bandwidth, regulation of service quality, optimization of coverage, security in WSNs, and additional sensor management responsibilities.

Cooperative games

In a cooperative game, participants have the ability to establish binding agreements. The objective is to minimize the overall energy usage of the Wireless Sensor Network (WSN) and extend its operational lifespan.

Non- Cooperative games

Non-cooperative game theory examines the strategies employed in interactions between rival players. Within this framework, a player is referred to as an agent, whose objective is to maximize their benefit by independently selecting their strategy. In essence, each participant in a non-cooperative game acts in their own self-interest while maintaining rational decision-making.

**The Prisoners' Dilemma Problem Scenario:**

Two employees at a company are caught in a corporate scandal, but the management lacks enough evidence to determine their involvement.

□ The management separates the two and offers both the same deal:

1. If one blames the other for the wrongdoing (betrays) while the other remains silent (cooperates), the accuser keeps their job with no penalties, while the silent employee is fired.

2. If both remain silent, they are given a warning and suspended without pay for one week.

3. If both blame each other (betray), they are both demoted and receive a pay cut for six months.

Each employee must independently decide whether to betray the other or remain silent, with their decision kept confidential. It is assumed that each employee's primary goal is to minimize their personal consequences.

The game transforms into a non-zero-sum scenario where the two players can choose to either cooperate or betray one another.

The intriguing symmetry of the problem lies in the fact that the optimal choice for each player is to betray the other, despite the fact that both would achieve a better outcome through mutual cooperation.

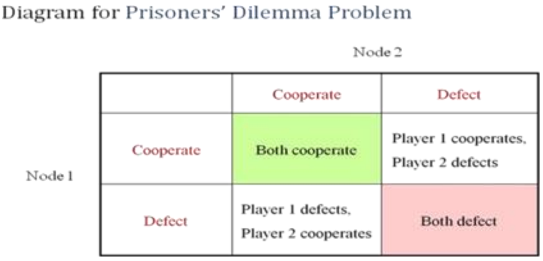
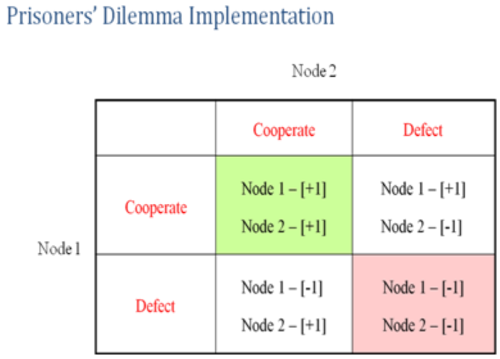


Diagram for Prisoners' Dilemma Problem

| | | Node 2 | |
|---|---|---|---|
| | | Cooperate | Defect |
| Node 1 | Cooperate | Both cooperate | Player 1 cooperates,<br>Player 2 defects |
| | Defect | Player 1 defects,<br>Player 2 cooperates | Both defect |

**Prisoner's Dilemma Problem**



Prisoners' Dilemma Implementation

| | | Node 2 | |
|---|---|---|---|
| | | Cooperate | Defect |
| Node 1 | Cooperate | Node 1 – [+1]<br>Node 2 – [+1] | Node 1 – [+1]<br>Node 2 – [-1] |
| | Defect | Node 1 – [-1]<br>Node 2 – [+1] | Node 1 – [-1]<br>Node 2 – [-1] |

**Prisoner's Dilemma Implementation**

## 4. PROPOSED WORK

□ Handling selfish behavior of sensor nodes in a WSN by using the game theoretic approach.

□ Assumption: [I] Assume detection of selfish behavior has been done.

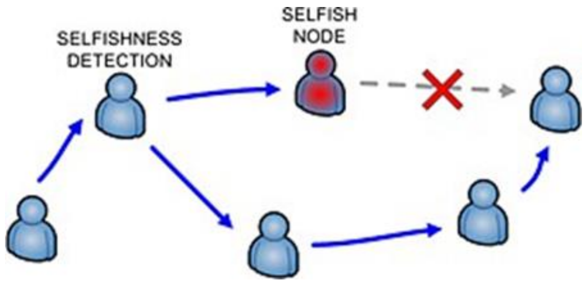


Fig: A Selfish Routing Scenario

## IV. Proposed Solution

We utilize the Prisoner's Dilemma framework, with bonus calculated as follows:

1. A cooperative node's bonus score increases by 1 for each packet it forwards.

2. When a non-cooperative node fails to forward a packet, its bonus score decreases by 1, while all other nodes'

scores increase by 1.

3. The network's minimum bonus threshold is a dynamic value, recalculated each time a packet travels from source to destination by determining the lowest bonus score among all nodes.

4. If a node's bonus score falls below the minimum threshold, it receives a penalty in the form of waiting time when acting as a source node. The duration of this Waiting period is inversely related to the node's bonus score.

**Algorithm: Selfish Routing**

```
Input: Network nodes, transmission packets
Output: Adjusted waiting time and bonus for each node
1. Initialize:
  - Set `bonus = 0` for all nodes in the network.
  - Activate `Watchdog` to detect selfish nodes in the network.
2. Packet Transmission:
  For each packet transmitted using AODV:
    a. Get the transmission path.
    b. Call `get_bonus()` to update the bonus values for nodes.
    c. Compute the packet transmission cost using `find_waiting_time()`.
  End For
3. Function: get_bonus()
  Input: Node `Ni` status (transmits/sends or not)
  Output: Updated `bonus` values for nodes.
  Begin:
    If Node `Ni` transmits:
      - Update `bonus[Ni] = bonus[Ni] + 1`
      - For all other nodes, no change.
    Else (Node `Ni` does not transmit):
      - Update `bonus[Ni] = bonus[Ni] - 1`
      - For all other nodes:
         - Update `bonus[node] = bonus[node] + 1`
    End If
  End Function
4. Function: find_waiting_time()
  Input: Updated `bonus` values for all nodes
```

```
Output: Computed waiting time for each node.
Begin:
  a. Identify the node with the minimum `bonus` value.
  b. Arrange nodes in ascending order based on their `bonus` values.
  c. For all nodes where `bonus[node] <= cutoff value`:
     - Set `waiting_time[node] = (1 / bonus[node]) * K`
End Function
```

**Results & Conclusion:**

In ad-hoc networks, nodes face limitations in communication range and battery life. This necessitates the use of intermediate nodes for data transmission. Nodes can be categorized as either cooperative or non-cooperative. Cooperative nodes function properly in relay networks, facilitating data transfer, while non-cooperative nodes exhibit selfish or disruptive behavior. To address routing misconduct, two mechanisms have been employed: Watchdog and Path rater. The Watchdog identifies misbehaving nodes by monitoring the next node in the path to ensure packet forwarding. It accomplishes this through promiscuous listening to the subsequent node's transmissions. If a node fails to forward a packet, it is deemed misbehaving. The Path rater utilizes this information to select network routes with the highest likelihood of successful packet delivery. A dynamic bonus monitoring system and node removal mechanism, based on game theory, have been proposed to manage selfish behavior in Wireless Sensor Networks (WSNs). Recent advancements in Game Theory (GT) for WSNs have been summarized. GT offers the ability to analyze numerous scenarios before taking action, enhancing decision-making processes. The potential for applying GT to WSNs is promising, with researchers exploring game-theoretic approaches to address WSN design challenges and proposing viable solutions.

**Future Research Directions:**

Even though a significant amount of study has already been done on the selfish routing problem of WSN, more effort must be done in order to find a worldwide solution. The list of possible research topics is as follows. The first efforts to identify misbehaving nodes and lessen their impact on performance in ad hoc wireless networks are presented in this paper. We outline some further concepts we would like to investigate in this section. To find the best values to boost throughput in various scenarios, we intend to carry out more thorough testing of the watchdog and path rater parameters. We are currently testing various watchdog criteria to determine when a node is acting inappropriately. In order to optimize certain variables for our simulations, we employ scenarios in

Our simulations use scenarios in which there are no *a pri*ori trust relationships, but we expect the performance of path rater to increase when it can make use of explicitly trusted nodes. Trusted node lists are available in some ad hoc network scenarios, and we would like to analyze the performance of our routing extensions in these scenarios. Currently the path rater only decrement a node's rating when another node tries unsuccessfully to send to it or if the watchdog mechanism is active and determines that a node is misbehaving. Without the watchdog active, the path rater cannot detect misbehaving nodes. An obvious enhancement would be to receive updates from a reliable transport layer, such as TCP, when ACKs fail to be received. This would allow the path rather to detect bad paths and lower the nodes' ratings accordingly. Hence, in our future work for handling selfish node behaviour in WSNs we plan to use incentive mechanisms.

**Refrences:**

[1] S.Marti, T.J. Giuili , K. Lai, and M. Baker , "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks" , in Proc. Int. Conf. Mobile Computing and Networking , Boston , MA , Aug. 2000 , pp. 255-265

[2] Shen, S., Yue, G., Cao, Q., Yu, F. A survey of game theory in wireless sensor networks security. *J. Netw. 2011, 6, 521–532.*

[3] Diman Zad Tootaghaj, Farshid Farhat, “Game-Theoretic Approach to Mitigate Packet Dropping in Wireless Ad-hoc Networks” IEEE Transactions on mobile computing , vol. 7 , no. 9 ,September 2008

[4] Lei Huang, Lixiang Liu, “Extended Watchdog Mechanism for Wireless Sensor Networks”, Proc. Workshop Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks Institute of Software, Chinese Academy of Sciences, May 2006 Vol.3, No. 1, 2008, *pp*. 39-48

[5]Aghaei, R. G., Rahman, M. A., Gueaieb, W. and Saddik, A. E., “Ant colony-based reinforcement learning algorithm for routing in wireless sensor networks,” in Instrumentation and Measurement Technology Conference (IMTC), Warsaw, Poland, 2007.

[6]Ahmed, N., Dong, Y., Bokareva, T. et al., “Detection and tracking using wireless sensor networks,” in Proceedings of the 2007 International Conference on Embedded Networked Sensor Systems, pp. 425–426, Sydney, Australia, November 2007.