A Survey on Security and Privacy Protocols for Wireless Sensor Networks using Cooperative Game Theory

Vinoba\(^1\), P. Hema\(^2\)

\(^1\)K.N. Government Arts College, Tamil Nadu, India
\(^2\)Assistant Professor, RMK CET

Abstract—In this paper, we focus on cooperative game theory between primary and secondary nodes via cluster heads. Each cluster head will send the request to the sub nodes of the respective groups and whichever node is registered within the request time is considered as primary users and others as secondary users. Cluster head use primary users which are having first priority for iteration items (say three times) based on Localization algorithm. After three iteration conditions primary users are treated as secondary users. Now, primary users will send data to the cluster heads, cluster head will transmit the data to the sink node. Meanwhile, secondary users will also send the data to the same cluster head and that specific cluster head will verify with neighbor cluster head (idle or not) so as to transmit the data delivered by secondary users to reduce the cluster head load during data transmission. Primary users will also move to the neighbor cluster head for data transmission where no need of registering in that cluster head using cooperative game theory. During mobility of nodes, misbehaving nodes is identified based on location ID. Lastly ranking is done based on energy level checking from all cluster heads and also we can identify the best cluster heads. Based on ranking process, secondary users move one cluster head to another cluster head for data transmission.

Keywords—Cooperative Game theory, Localization algorithm network security, Primary node, Secondary node.

I. INTRODUCTION

Wireless Sensor Networks is an emerging technology which plays a vital role in most of the important applications. The mode of operation in sensor network consists of a large number of sense nodes for communication. These sensor nodes are able to sense the information from one end transmitter side and process it and send it to the selected destinations. Wireless sensors have characteristics behaviors such as macro dimension, very low cost, highly reliable, flexibility to install anywhere and low energy consumption. Because of these energy saving behaviors, they could be deployed in various fields such as oil fields, military, defense, agricultural, industrial, and biomedical and many more real and non real time application domains [1].

The sensor they could easily be used in different environments such as unmanned and critical regions. So the cost of network is less, complicated configuration and installation for these sensors in the network connects each other, we could use them with lesser cost in comparison with traditional or commercial networks. Our research efforts focused on establishing efficient routing paths for transmitting packets from a sensor node to a sensor destination [2]. Routes to find the best and well selected profitable way for data transmission from source node to the destination node in the network by considering different parameters (e.g. flexibility, reliability, overhead, throughput, stability, consumed and wasted power, data speed, etc). Our proposed sensor parameters to increase the wireless sensor networks Lifetime. Lifetime is one of the most important factors of deployed wireless sensor networks. Finding the best shortest route length to reduce the transmission overhead and reduced delay time. To increase the ratio of packets in packet delivery fraction, these wireless sensor networks must be designed and used in an efficient way to optimize the sensor to reduced power consumption and increased life time of the sensor network player. Our idea to proposed work, using probability selection Game Theory approach for WSN, optimal discovery of route in WSN is discovered. Our approach towards this proposed project, we developed network to select route based on routing and sensor nodes the same things are assumed to be the game and players of the networks respectively. Each and every node in the network we considered wants to increase their benefit in the present network. So we use a different mixed strategy model as well as network profit and loss calculation for each player that alive in the networks. In this proposed method, the destination node player node pays a recognition to the source player node for each data packet successfully reception from the source player to destination player. Moreover, the source player pays attention of this credit to each intermediate player node or relay player node that participates in sending data packet transaction. Yet to decide, each node sustains a transmission cost for each data packet transaction to other intermediate or destination receiving node.
The cost is called networks Transmission Cost or path loss and related to different type of parameters. Each player transmits the received data packet to the next or intermediate hop with the selected player game probability, calculated by the reliability of the multiple player that playing in the network. Our enhanced parameter checked on player characteristics or behaviour, e.g. link error checking, probability, duty cycle, etc.

II. RELATED WORKS

Relatively, a number very limited of works was done in the sector of Unlicensed/Licensed wireless sensors networks. Most of them concentrate upon one side of CWSN challenges. Some of them try to introduce the attacks which threaten CWSN. Just handful research works presented integrated mechanisms to face most challenges. In an energy-efficient and adaptive modulation technique is introduced for CWSN in order to achieve high power efficiency to maximize the lifetime of sensor networks. Previous works about security in CR presented to analyze the effects emerged by Unlicensed/Licensed features and how they could be used to reduce the negative effects. In the article [8] each characteristic of CR - the three main characteristics are: environment awareness, learning and acting capacity - and the attacks that could take advantage of it are analyzed. Provide threats that affect the ability to learn of Unlicensed/Licensed networks and the dynamic cluster access. The article present a new secure cluster sensing protocol, it bases its functionality on the generation and transmission of specific keys to each node. Jamming attacks have special characteristics in Unlicensed/Licensed networks, article shows a countermeasure based on frequency hopping to avoid this kind of attacks. The definition of the primary user emulation (PUE) attacks was introduced by Chen and Park in and they focused in on countermeasures against PUE. Securing CR networks is well-introduced in many articles such as without taking into account the special characteristics of WSN. Also, much more articles discuss security in WSNs but do not use Unlicensed/Licensed capabilities. In these days, very little works focus on security in CWSN. For this reason, we have to concentrate more in this topic.

III. COOPERATIVE GAME THEORY

Game theory provides a mathematical basis for the analysis of interactive decision-making processes. It provides tools for predicting what might happen and possibly what should happen when agents with conflicting interests interact.

It is not a single monolithic technique, but a collection of modeling tools that aid in the understanding of interactive decision problems.

A cooperative game is a game in which the players have complete freedom of pre play communication to make joint binding agreements. These agreements may be of two kinds to coordinate strategies or to share payoffs.

In non-cooperative game theory, we focus on the individual player’s strategies and their influence on payoffs and try to predict what strategies players will choose (equilibrium concept).

In cooperative game theory, we abstract from individual player’s strategies and instead focus on the coalition players may form. We assume each coalition may attain some payoffs, and there we try to predict which coalitions will form (and hence the payoffs agents obtain).

Under cooperative games, players can coordinate their strategies and share the payoff. In particular, sets of players, called coalitions, can make binding agreements about joint strategies, pool their individual agreements and, redistribute the total in a specified way. Cooperative game theory applies both to zero-sum and non-zero-sum games.

Cooperative theory starts with a formalization of games that abstracts away altogether from procedures and . . . concentrates, instead, on the possibilities for agreement. . . . There are several reasons that explain why cooperative games came to be treated separately. One is that when one does build negotiation and enforcement procedures explicitly into the model, then the results of a non-cooperative analysis depend very strongly on the precise form of the procedures, on the order of making offers and counter-offers and so on. This may be appropriate in voting situations in which precise rules of parliamentary order prevail, where a good strategist can indeed carry the day. But problems of negotiation are usually more amorphous; it is difficult to pin down just what the procedures are. More fundamentally, there is a feeling that procedures are not really all that relevant; that it is the possibilities for coalition forming, promising and threatening that are decisive, rather than whose turn it is to speak.. Detail distracts attention from essentials. Some things are seen better from a distance.

IV. OUR PROPOSED SCHEME

The proposed scheme is inspired from the inspection game, a game theory model in which an inspector verifies if another party, called inspectee, adheres to certain legal rules.
In this model, the inspectee has a potential interest in violating the rules while the inspector may have to perform the partial verification due to the limited verification resources. Therefore, the inspector could take advantage of partial verification and corresponding punishment to discourage the misbehaviors of inspected. Furthermore, the inspector could check the inspectee with a higher probability than the Nash Equilibrium points to prevent the offences, as the inspectee must choose to comply the rules due to its rationality. Inspired by inspection game, to achieve the tradeoff between the security and detection cost, we model the inspection game and use game theoretical analysis to demonstrate that cluster head could ensure the security of node routing at a reduced cost via choosing an appropriate investigation probability. The contributions of this paper can be summarized as follows: We also discuss how to correlate a user’s reputation (or trust level) to the detection probability, which is expected to further reduce the detection probability.

V. Algorithm Definition

*Localization Algorithm:* Localization is an algorithm for robots to localize using a particle filter. Given a map of the environment, the algorithm estimates the position and orientation of a node as it moves and senses the environment. The algorithm uses a particle filter to represent the distribution of likely states, with each particle representing a possible state, i.e., a hypothesis of where the node is.[1] The algorithm typically starts with a uniform random distribution of particles over the configuration space, meaning the robot has no information about where it is and assumes it is equally likely to be at any point in space. Whenever the node moves, it shifts the particles to predict its new state after the movement. Ultimately, the particles should converge towards the actual pose of the node.

VI. Data Flow Diagram

- **NO OF USERS (PRIMARY & SECONDARY USERS)**
- **FORM CH1….CH-N**
- **USER REGISTRATION BASED ON REQUEST**
- **DATA TRANSMISSION BASED ON PRIORITY USING THRESHOLD VALUE**
- **LOAD BALANCING (CLUSTER HEAD TO CLUSTER HEAD HANDOVERING REDUCE WAITING TIME)**
- **WHICH CLUSTER HEAD HAS MAXIMUM ENERGY**
- **USERS ARE MOVES ONE CLUSTER HEAD TO ANOTHER CLUSTER HEAD BASED ON RANKING USING COOPERATIVE GAME THEORY**
- **IDENTIFY MISBEHAVIOR USER BASED ON LOCATION ID USING LOCALIZATION ALGORITHM**
- **RANKING PROCESS**
- **SINK**
VII. SIMULATION SCENARIO

VIII. SIMULATION TABLE RESULT

Simulation setup:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Size</td>
<td>1900x1100</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>100</td>
</tr>
<tr>
<td>Range</td>
<td>500m (300m – 600m)</td>
</tr>
<tr>
<td>Throughput</td>
<td>6 Mbps (9.0 Mbps, 20 Mbps)</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>3.0 Mbps</td>
</tr>
<tr>
<td>Frequency</td>
<td>5 Hz</td>
</tr>
<tr>
<td>Average Speed of nodes</td>
<td>6.0 m/s</td>
</tr>
<tr>
<td>Data Transmission</td>
<td>1200 Bytes</td>
</tr>
<tr>
<td>Packet Rate</td>
<td>200 Packets per second (pps)</td>
</tr>
<tr>
<td>Request message interval</td>
<td>10 – 50 Seconds</td>
</tr>
<tr>
<td>Mobility Factor</td>
<td>200 seconds</td>
</tr>
<tr>
<td>Initial Energy Assigned</td>
<td>100 Joules</td>
</tr>
<tr>
<td>Energy Consumption</td>
<td>40 Joules</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>600 seconds</td>
</tr>
</tbody>
</table>
IX. CONCLUSION

We also discuss how to correlate a user’s reputation (or trust level) to the detection probability, which is expected to further reduce the detection probability. Primary users will also move to the neighbor cluster head for data transmission where no need of registering in that cluster head using cooperative game theory. During mobility of nodes, misbehaving nodes is identified based on location ID. Lastly ranking is done based on energy level checking from all cluster heads and also we can identify the best cluster heads. Based on ranking process, secondary users move one cluster head to another cluster head for data transmission.
REFERENCES


