IJASRM

International Journal of Advanced Scientific Research and Management, Vol. 1 Issue 2, February 2016.

www.ijasrm.com

COGNITIVE MODEL FOR IDENTIFICATION OF MALICIOUS SENSOR NODE BEHAVIOR

[1]Devaraj Verma C, [2]Dr. M V Vijayakumar and [3]Pooja K Swamy.

[1]Research Scholar, NHCE(VTU) & Assistant Prof, Dept of MCA, DSCE,
Bangalore, Karnataka, India -78

[2]Professor, Dept of CSE, Dr. AIT,
Bangalore, Karnataka, India -72.

[3]Student, Dept of ISE, PESIT,
Bangalore, Karnataka, India -85.

Abstract

Wireless sensor networks [1-2] is a technology which as a diverse number of applications. While these networks are infrastructure less and do not have any public address. They are made up of many tiny sensor nodes and have insecure radio links. Thus they are highly vulnerable to security threats since the sensor nodes are the core weakness as they are with limited-resource. This paper aims at mitigating the security threats [7] to the wireless sensor network by implementing the reinforcement Q learning algorithm [4-6]. A new intrusion detection system called the Markovian [1] IDS is designed, to protect sensor nodes from malicious attacks. The Markovian IDS incorporates Q learning [4-6] to sense the network and attributes of each nodes.

Keywords: *Q-learning, MDP, Cognitive Model, Security Threats.*

1. INTRODUCTION

The main objective of this research paper is to build a test-bed for detecting and alerting about the abnormalities of the malicious sensor nodes[1] using the Q learning technique[2, 4, 5, 6] and Markovian Decision Process (MDP) [1, 7]. The test-bed generates random sensor network and real time abnormalities to the sensor nodes which is made highly user friendly for the demonstration from purpose.

The investigation of the model aims at the following:

- Integrating the cognitive mind into a networking world
- Designing, testing and performing computational analysis on simple and complex minds.
- Reflexive behavior, goal-oriented behavior and self maintenance are the main behaviors considered in the cognitive agents.
- Agents are designed to perform their task in a dynamic environment.
- Various types of malicious behaviors are considered for detection of the malicious behavior in the sensor networks.

2. RESEARCH SCOPE

The scope of the research investigation is to build a test bed that demonstrates real time sensor node abnormality detection. This will help the artificial intelligent researcher to use the model for the analysis of the intruder detection and how the source code can be implemented on cluster heads or base stations for real time malicious node detection.

3. SYSTEM DESIGN

The investigation of the cognitive model for false node identification consists of four major components or modules:

- **Graphical User Interface (GUI)**:

This module provides user with options to generate a random sensor network and agents, to perform attack and detect for attack.

- **Training**:
  This module trains the agents to sense the environment, determination of the location of sensor nodes, and calculations for the q-values based on it location.
- **Markovian DecisionProcess**:
  This module determines the reward and punishment for each action and thus decides on the path to traverse from the gathered information.
- **Detection**:
  This module is responsible for the agents to detect the malicious behavior of each node in the sensor network and raise alter for the same.

The proposed cognitive model for detecting unintended node uses a generic cognitive architecture [3] and is developed in terms of generic cognitive and meta-cognitive agent types [3]. It aims at modeling the cognitive abilities, function and mechanisms such as planning, optimal decision making, problem solving and learning in the agents. The agents are categorized into: (1) reflexive agent (2) reactive agent (3) deliberative agent and (4) learning agent. Thus, the model is built on four layers as shown in the Fig 1 where each high layer uses its lower layer for the basic functionalities.

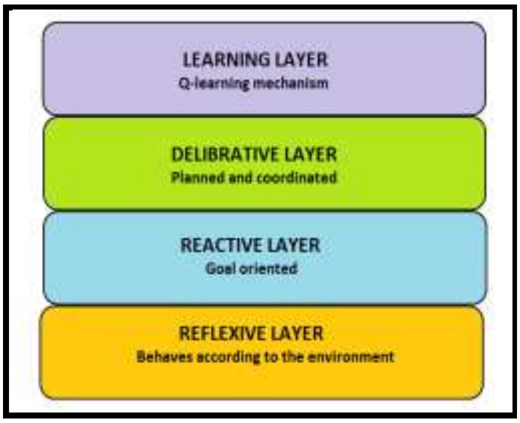

Fig 1 Cognitive Model for Malicious Node Detection

REFLEXIVE AGENTS

The human and animal biological neuromuscular action derives the reflex actions. These built-in reflexes can occur quickly even before thinking. Explicit motivational states like Belief, Desire and Intentions do not exist in these types of agents. These agents in response to the immediate environment in front of it moves in one of the four directions (left, right, up, down) to move into the free-space and away from obstacles. Navigating in the environment without colliding with other agents in the environment is the main task of these agents. Fig 1.2 shows the structure of a reflexive agent.

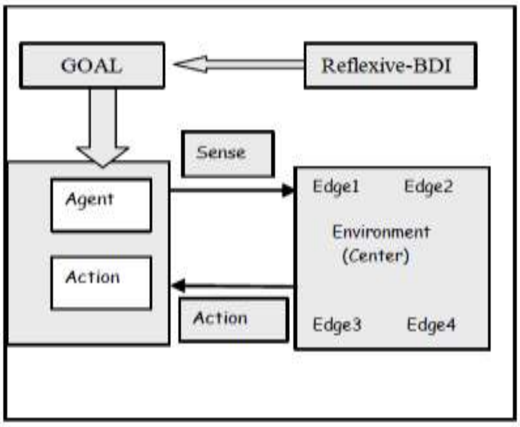

Fig 1.2 Structure of reflexive agent.

REACTIVE AGENTS

These agents work with more flexible control mechanism. They integrate decision making and behaviors. These are goal oriented agents whose behavior is built on the reflexive agents. Their goal is to discover the resource, then make a move to the nearest resource in the shortest path and to collect or check the resource (collects energy units and check sensor nodes behavior). Fig 1.3 shows the structure of reactive agents.

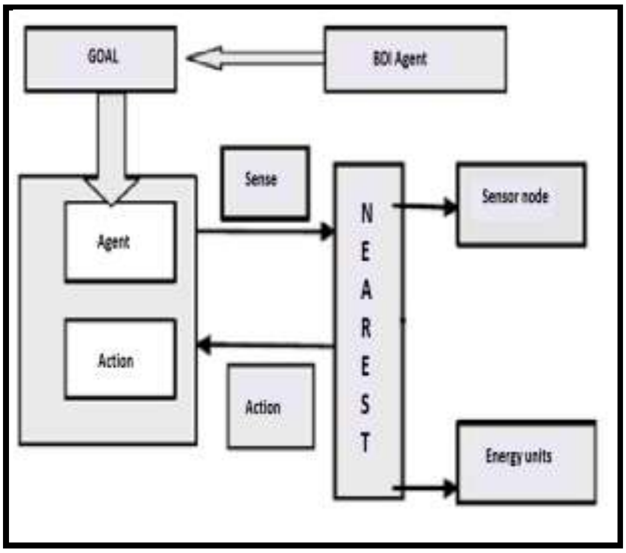

Fig 1.3 Structure of reactive agent.

DELIBERATIVE AGENTS

These agents are built using behaviors of both reflexive agents and reactive agents. They are planned and coordinated agents. They are capable of altering the reflexive and reactive agents and are also capable of maintaining their internal state such as energy level of the agents. Fig 1.4 shows the structure of deliberative agent.

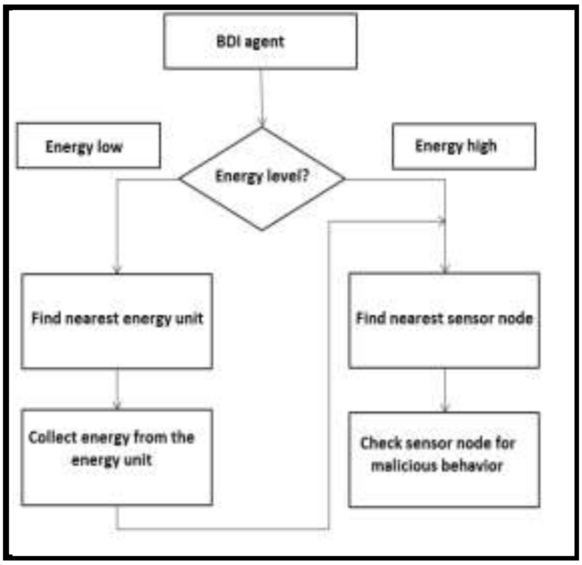

Fig 1.4 Structure of deliberative agent.

LEARNING AGENTS

These agents aim at maximizing the total rewards in the architecture. How to maximize the total reward is derived by the value function.

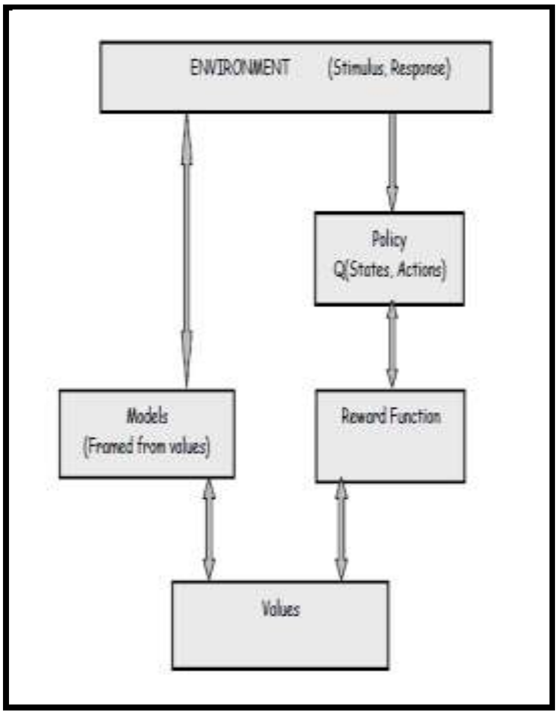

Fig 1.5 Q-learning mechanism

The application of q-learning maximizes the visit to sensor nodes for checking their behavior. Fig 1.5 shows the q-learning mechanism used by the learning agents.

ATTACKS CONSIDERED

The Cognitive Model for Multi-agent IDS is designed to identify the following types of attacks. Table 1 shows the different types of attacks considered and their affects on the parameters.

TABLE 1 TYPES OF ATTACKS

Type of Attack	Attributes	Normality	Abnormality
Voltage drained	Voltage	3.7 V	Less than 2.5 V Greater than 4.26 V
TCP Xmas	TCP_FIN TCP_URG TCP_PUSH	0 0 0	1 1 1
TCP_FIN Flood	TCP_FIN	0	1
Ping of Death	ICMP_SIZE	2^16 bytes	Larger than 2^16 bytes
TCP ECE Flood	TCP_ECE	0	1
Twinge trash	ICMP_TYPE ICMP_CODE	0-255 0-40	Greater than 255 Greater than 40
Packet rate	Packet_rate	10bps	Greater than 10bps
Buffer Overflow	Buffer_size	12	Greater than 12

4. RESULTS AND DISCUSSIONS

Each type of agents is experimented independently in the test bed developed. The life expectancy and performance statistics are compared for each agent. Each agent is experimented for the same time scale and same network topology. An average of 10 experiments is considered, to manage consistency, and avoid variations of the simulated results. The results are then plotted into a graph. The Learner agent maintains the highest performance as well as the life expectancy rate. Random agent checks 16% of the sensor node, Reflexive agent checks 26% of the sensor node, Learner agent checks 80% of the sensor node.

5. CONCULSION

This work has integrated the field of artificial intelligence and cognitive science with networking to develop the cognitive model for finding the unwanted node behavior in the intelligent IDS system. It demonstrates how an intelligent mind can work at detecting malicious nodes in the networking environment. This work is developed based on the concept of cognition. The Model developed with the following features: (1) remedial action (2) self-regulation (3) schema training. The experimental testing as proven that learner agent maintains a higher level of life expectancy than the other agents and high number of sensor nodes checked than other agents.

6. REFERENCES

[1] Jen-Yan Huang , I-En Liao, Yu-Fang Chung , Kuen-Tzung Chen "Shielding wireless sensor network using Markovian intrusion detection system with attack pattern mining" Information Sciences Volume 231: 32–44, 10 May (2013).

[2] Dr. G. Padmavathi, Mrs. D. Shanmugapriya " A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" (IJCSIS) International Journal of Computer Science and Information Security.Vol. 4, No. 1 & 2, (2009).

[3] M.V Vijayakumar, "Society of Mind Approach to Cognition and Metacognition in a Cognitive Architecture", PhD Thesis, University of Hull, UK, (2008).

[4] Shahaboddin Shamshirband, Ahmed Patel, Nor Badrul Anuar, Laiha Mat Kiah, Ajith Abraham, "Cooperative game theoretic-approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks", Engineering Applications of Artificial Intelligence 32: 228–241,(2014).

[5] Richard S. Sutton and Andrew G. Barto "Reinforcement Learning: An Introduction", A Bradford Book, MIT Press, Cambridge, MA, (1998).

[6] Martijn van Otterlo and Marco Wiering, "Reinforcement Learning and Markov Decision Processes".Website: http://www.ai.rug.nl/~mwiering/Intro_RLBOOK.pdf

[7] Seo Hyun Oh, Chan O. Hong, Yoon-Hwa Choi," A Malicious and Malfunctioning Node Detection Scheme for Wireless Sensor Networks ",Wireless Sensor Network, Vol 4: 84-90, (2012).