Applied Soft Computing 19 (2014) 68–79

Contents lists available at ScienceDirect

Applied Soft Computing

journal homepage: www.elsevier.com/locate/asoc

Swarm intelligence based approach for sinkhole attack detection in wireless sensor networks

N.K. Sreelaja [a,*], G.A. Vijayalakshmi Pai [b,1]

[a] Sri Krishna College of Engineering and Technology
[b] PSG College of Technology, Coimbatore, India

ARTICLE INFO

Article history:
Received 26 December 2009
Received in revised form 10 June 2012
Accepted 18 January 2014
Available online 2 February 2014

Keywords:
Artificial intelligence
Ant Colony Optimization
Boolean expression minimization
Message authentication

ABSTRACT

Swarm intelligence, a nature inspired computing applies an algorithm situated within the context of agent based models that mimics the behavior of ants to detect sinkhole attacks in wireless sensor networks. An Ant Colony Optimization Attack Detection (ACO-AD) algorithm is proposed to identify the sinkhole attacks based on the nodeids defined in the ruleset. The nodes generating an alert on identifying a sinkhole attack are grouped together. A voting method is proposed to identify the intruder. An Ant Colony Optimization Boolean Expression Evolver Sign Generation (ABXES) algorithm is proposed to distribute the keys to the alerted nodes in the group for signing the suspect list to agree on the intruder. It is shown that the proposed method identifies the anomalous connections without generating false positives and minimizes the storage in the sensor nodes in comparison to LIDeA architecture for sinkhole attack detection. Experimental results demonstrating the Ant Colony Optimization approach of detecting a sinkhole attack are presented.

1. Introduction

A swarm intelligent system is essentially a simple agent based model consisting of a huge number of simple agents interacting with each other and some environment. The field of artificial life produced a number of models based on "swarms" of simple agent rules capable of producing a higher-level identity, such as the insect colonies behavior. Swarm intelligence [17] is an algorithm that models the collective behavior of social insects. Here, an autonomous agent is a subsystem that interacts with its environment, which probably consists of other agents, but acts relatively independently from all other agents. The autonomous agent does not follow commands from a leader, or some global plan [3]. Natural examples of Swarm Intelligence include ant colonies, bird flocking, animal herding, bacterial growth, and fish schooling. Ant system is a swarm intelligence algorithm to solve optimization problems. Artificial ants [11] have some characteristics which do not find counterparts with real ants. They live in a discrete world and the moves consist of transitions from discrete state to discrete states. They have an internal state. This private state contains the memory of the ant agent's past action. They deposit a particular amount of pheromone, which is a function of the quality of the solution found. An artificial ant's timing in pheromone deposition is problem dependent and often does not reflect real ant's behavior.

Swarm intelligence based techniques can be used in a number of applications such as controlling unmanned vehicles, controlling nanorobots within the body for the purpose of killing cancer tumors [7], telecommunication networks, mobile media [12], and intrusion detection. This paper focuses the application of swarm intelligence algorithm (Ant Colony Optimization) to detect sinkhole attacks in a wireless sensor networks.

A Wireless Sensor Network (WSN) is a network of cheap and simple processing devices (sensor nodes) that are equipped with environmental sensors for temperature, humidity, etc. and can communicate with each other using a wireless radio device. They are composed by a large amount of tiny sensing devices which are very limited in energy, computation, and communication capabilities. The need for administration and utilization of wireless sensor nodes arise because of the unattended operation of a large number of sensor nodes in many applications. Encryption and authentication mechanisms provide reasonable defense only for remote-class outsider attacks [6]. This is because an insider is allowed to participate in the network and have complete access to any messages routed through the network and is free to modify, suppress, or eavesdrop on the contents. To overcome this, intrusion detection techniques are used to detect third party break in attempts.

Wireless sensor networks are vulnerable to sinkhole attacks as they have special communication pattern. All sensor nodes send

* Corresponding author.
E-mail addresses: sreelajank@gmail.com (N.K. Sreelaja), paigav@mca.psgtech.ac.in (G.A. Vijayalakshmi Pai).
[1] Tel.: +91 422 2572177/2572477; fax: +91 422 2573833.

1568-4946/$ – see front matter © 2014 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.asoc.2014.01.015

packets to the base station. Sensor nodes in the same area are affected even if only one compromised node is providing a high quality route to the base station. A sinkhole attack is a severe attack that prevents the base station from obtaining complete and correct sensing data, thus forming a serious threat to higher layer applications. Sinkhole attack is difficult to detect because simply using user authentication and signed routing information cannot prevent compromised nodes from generating signed routing packet with wrong information. To launch a sinkhole attack, an adversary lures nearly all traffic from a particular area through a compromised node. The adversary usually attracts network traffic by advertising itself as having the shortest path to the base station and can then tamper packets originated from any nodes in the area.

Da Silva et al. [2] and Onat and Miri [10] have proposed two similar Intrusion Detection Systems (IDS), where certain monitoring nodes in the network are functioning as watchdogs for their neighbors, looking for intruders. They listen to messages in their radio range and store in a buffer specific message fields that might be useful to an IDS running within a sensor node, but the working of the system is not explained. In these architectures, there is no collaboration among the monitor nodes. Ioannis et al. [5] has concluded from both papers that the buffer size is an important factor that greatly affects the rate of false alarms. Ngai et al. [9] has proposed an approach on the intrusion detection of sinkhole attacks. However, this approach involves the base station in the detection process, resulting in a high communication cost for the protocol. Dallas et al. [1] proposed a hop count method to detect sinkhole attacks. This technique assumed static network topology and hop-count distribution exhibit lognormal distribution. These assumptions might not hold in a real world sensor networks deployment, and the technique might not perform well.

To overcome the drawbacks of these approaches Ioannis et al. [5] has proposed LIDeA architecture for detecting sinkhole attack in a wireless sensor network. In their model, all sensor nodes are loaded with an IDS agent and they dynamically become activated around the attacking node and collaborate in order to isolate it from the network. The drawback of LIDeA architecture is that they do not discuss on how to detect sinkhole attacks, although rule patterns are described for defending against sinkhole attacks. Also the number of keys to be stored by each alerted node depends on the number of alerted nodes in the group thereby leading to an increase in storage.

Though the rule matching method used to detect sinkhole attack is not specified in LIDeA architecture, the classical approaches proposed in literature for detecting attacks based on rule match is studied and found to have some drawbacks. Salameh et al. [16] proposed a Neural Network (NN) based approach for detecting attacks based on the rules in the ruleset. The network is trained using a backpropogation learning rule to identify attacks. The drawback of the scheme by applying it to detect attack is that it generates false positives. Mukkamala et al. [8] proposed a Support Vector Machine (SVM) based approach for detecting attacks based on rules in the ruleset. The drawback of this method is that it generates false positives.

In this paper, a swarm intelligence based (Ant Colony Optimization) intrusion detection for sinkhole attacks in wireless sensors is proposed. The first phase of the work discusses about generating alerts by the sensor nodes in the wireless sensor network on detecting sinkhole attacks by a rule matching method using an Ant Colony Optimization based approach. An *Ant Colony Optimization based Attack Detection* (*ACO-AD*) algorithm is proposed to generate alerts by the sensor nodes of the wireless sensor networks based on the nodeids and the link quality defined in the ruleset. The second phase of the work discusses about identifying the intruder using a voting analysis method. Each alerted node transmits the suspect list of nodeids to the neighboring alerted nodes to agree on the intruder. The suspect list sent by the alerted node is signed using a key. An Ant Colony Optimization approach of obtaining minimized Boolean expression is used to generate minimum number of keys for signing the suspect list. An Ant Colony Optimization Boolean Expression Evolver Sign Generation (ABXES) algorithm is proposed to distribute the keys to the alerted nodes to sign the suspect list. The alerted nodes on receiving the suspect list count the occurrence of each nodeid in the suspect list. The nodeid having the highest count is identified as the intruder.

The advantage of the proposed method using Ant Colony Optimization for intrusion detection is that the sensor nodes generate alerts based on the nodeids in the ruleset without generating false positives. Also each alerted sensor node stores log n keys for verifying the authenticity of the suspect list using an ACO approach. Thus the storage in each alerted sensor node is minimized when compared to the one-way hash chain function approach used in Light Weight Intrusion Detection Architecture (LIDeA) approach to detect the intruder node. The number of searches using ACO-AD algorithm for matching the nodeid in the sender field of the packet with the nodeids in the ruleset is less when compared to the existing rule matching approaches.

Section 2 describes Ant Colony Optimization. Section 3 describes intrusion detection model architecture. Section 4 details Ant Colony Optimization based rule matching for sinkhole attack detection. Section 5 explains the voting method for identifying the intruder node. Section 6 explains a case study for intruder detection. Section 7 discusses the experimental results. Section 8 shows the comparison between ACO based methods of intrusion detection of sinkhole attack with the existing methods. Section 9 discusses the conclusion.

2. Ant Colony Optimization

A colony of ants denoting a set of computational concurrent and asynchronous agents moves through states of the problem corresponding to partial solutions of the problem to solve. They move by applying a stochastic local decision policy based on two parameters, called *trails* and *attractiveness*. By moving, each ant incrementally constructs a solution to the problem. When an ant completes a solution, or during the construction phase of the solution, the ant evaluates the solution and modifies the trail value on the components used in its solution. This pheromone information will direct the search of the future ants. Furthermore, an ACO algorithm includes two more mechanisms such as *trail evaporation* and, optionally, *daemon actions*. Trail evaporation decreases all trail values over time, in order to avoid unlimited accumulation of trails over some component. Daemon actions can be used to implement centralized actions which cannot be performed by single ants, such as the invocation of a local optimization procedure, or the update of global information to be used to decide whether to bias the search process from a non-local perspective [15].

3. Intrusion detection model architecture

To detect a sinkhole attack, each sensor node has IDS. There are several modules which determine the functioning of IDS. These include Local Packet monitoring module, Local detection engine, Cooperative detection engine and Local Response module. The Local Packet monitoring module gathers audit data by listening to its neighboring nodes.

Based on the rules defined to detect a sinkhole attack, the local detection engine of each sensor node has a ruleset which has the nodeids of its neighboring sensor nodes along with the link quality of each node detected using the local packet monitoring system by listening to the neighboring nodes transmission. The ruleset does not have the nodeid of the sensor node in which the IDS is present [4]. Table 1 shows the nodeids in the ruleset. The nodeids are sorted