An Intrusion Detection Framework for Sensor Networks Using Honeypot and Swarm Intelligence

Rajani Muraleedharan, and Lisa Ann Osadciw

Department of Electrical Engineering and Computer Science
Syracuse University, Syracuse, NY- 13244-1240
Phone: 315-443-3366/Fax: 315-443-2583
{rmuralee, laosadci}@ecs.syr.edu

Abstract -Wireless Sensor Networks have become a technology for the new millennium with the endless possibilities for applications ranging from academic to military. These tiny sensors are deployed in open environments, where security for data or hardware cannot be guaranteed. Unfortunately due to the resource constraints, traditional security schemes cannot be applied. Therefore designing protocols that can operate securely using smart inherent features is the best option. In this paper, an efficient way of detecting an intruder using Honeypot and Swarm Intelligence is proposed. The Honeypot architecture strategically enables agents to track the intruders. This process of locating an intruder reduces the false alarm detection rate caused by Denial-of-service attacks. A detailed analysis of the attack is captured to predict future attacks using pattern recognition. The proposed framework is evaluated based on accuracy and speed of intruder detection before the network is compromised. This process of detecting the intruder earlier helps learn his/her future attacks, but also a defensive countermeasure.

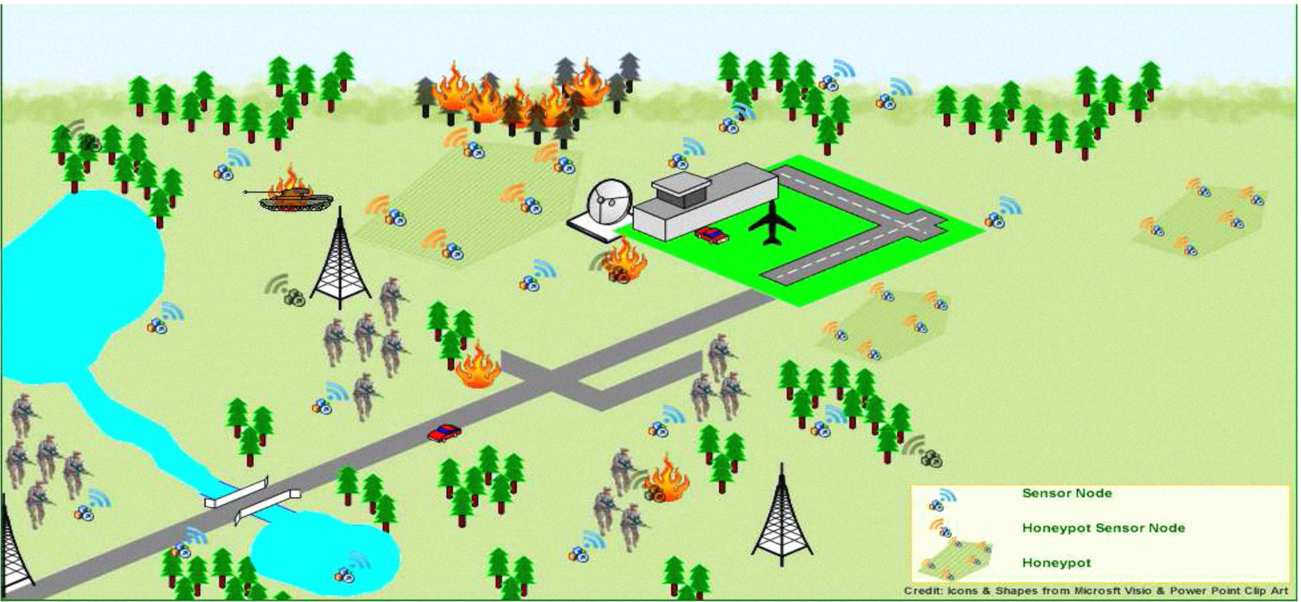
Keywords: Denial of Service, Honeypot, Intrusion Detection, Security, Swarm Intelligence, Wireless Sensor Network.

I. Introduction

The recent growth in networking technology demands a secure, reliable and cost effective wireless sensor network (WSN). Some of these networks lack security due to resource constraints, such as power, bandwidth and memory, thus, resulting in reduced Quality of Service (QoS). A network or node can be affected by several types of denial-of-Service (DoS) attacks including those forcing nodes to be in an idle or stand-by mode[3]. In this paper, heterogeneous sensors with varied type and functionality such as, camera sensors, seismic sensors, heat sensors, temperature sensors and biosensor are deployed in a region of interest. Due to the sensor's varied functionality the security breach at each node could affect the overall performance of the application.

II. Battlefield Monitoring

Battlefield monitoring system is initialized secretly by deploying sensors in a random manner using UAVs. Figure 1 illustrates two types of network deployed in securing battlefield monitoring. Apart from the sensors monitoring the battlefield, the honeypot sensors are also deployed, where they are primarily used as bait for intruders. Honeypot sensors are used to strategically mimic the "data" relayed within the real application. The shaded sensors in Figure 1 are honeypot sensors, where the message traffic is induced. The perfor-



Credit: Icons & Shapes from Microsft Visio & Power Point Clip Art

Fig. 1. Battlefield Monitoring Using Honeypot Architecture

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2009.7084
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2009.7084

mance of the network is influenced by quality of data collected and processed by sensor, but also the amount of time required to be transmitted to base (destination).

The chosen route needs to be resource optimal and energy efficient where the network is faced with issues such as fading, transmission error and attacks by intruders. The agents ensure the optimal route is taken to the destination using limited resources and also learning the network environment. Initially, the computational cost and time is high but this drops drastically once the agents learn the network and environment. Due to space limitation, a more detailed description can be obtained from our previous work (cognitive protocol) [3, 4].

III. Honeypot Framework

Wireless networks are prone to attacks in every layer [2] and complex traditional security measures are not attractive solutions. Due to the existing resource constraints in sensor nodes, there are two possible ways of protecting the network, a) Honeypot framework and b) Countermeasure using SI upon detecting an attack. The latter is discussed in [4]. Our approach can promise the following features in WSN: 1. Adaptive QoS features, 2. Traffic Prioritization, 3. Secure and energy-efficient routing, 4. Anomaly based detection and 5. Improve accuracy of detection rate i.e., reduce False positive claims.

III.a Honeypot

Honeypot mimics the biological nature of a particular species of ant, 'honey ants', where food is stored in them and thus form a living repository of food source. Due to their nature of work they are often attacked by raiders who pillage for the food repository. This natural phenomenon was successfully adapted to modern day intruders in computational networks. For example, World Wide Web, uses Honeypot to track a hacker [5, 6], where dedicated nodes are used.

Similarly, in WSN, a Honeypot network can be implemented using 'honey ants' as energy is inevitable. Hence, there are two types of agents involved in the network, one that communicates normal traffic, and another that stores virtual traffic but closely monitored for any request from intruders. There are two types of Honeypot, a) low-interaction, which only monitors for any anomalies and b) high-interaction, where detailed information of the requests are used for predicting future attacks using pattern recognition. The information senstivity, resources and time are the most important factors in choosing the type of Honeypot for any application.

III.b Implementing Honeypot Using SI

Figure 2 illustrates the implementation of Honeypot framework. The network comprises of both genuine sensor nodes that are either in active relay status or idle and honey-nodes i.e., honey agents that contain virtual comunication. When the information of the person or object of interest is captured by the nodes, the data is communicated to the destination (database) node, where the decision of whether its a normal activity (acceptance) or a terrorist activity (rejection) is made. Simultaneously, an intruder trying to gain access to the network is shown using 3 bold arrows. The intruder tries to communicate to his/her neighboring nodes which are active, but seldom does he know that his actions are been recorded and tracked using SI.

The nature of swarm agents sharing of local information with its neighbors can be strategically used to the user's advantage to trap the intruder using "virtual" trails. Since the Honeypot does not receive any traffic from genuine nodes any benevolent traffic can be removed using the Tabu-list feature of SI. The architecture is modelled based on game theory. The swarm agents, uses pheromone deposition as the means of communication, the higher pheromone value relates to the higher probability of route selection. This feature plays an important role in deceiving the intruder by creating virtual values along the Honeypot network. Hence, an intruder who is watching the traffic would assume everything is normal and end up attacking or probing the Honeypot network. Also, SI is used as an optimization algorithm. Thus, the process of tracking the intruder while balancing the virtual and real resources and traffic prioritization is possible.

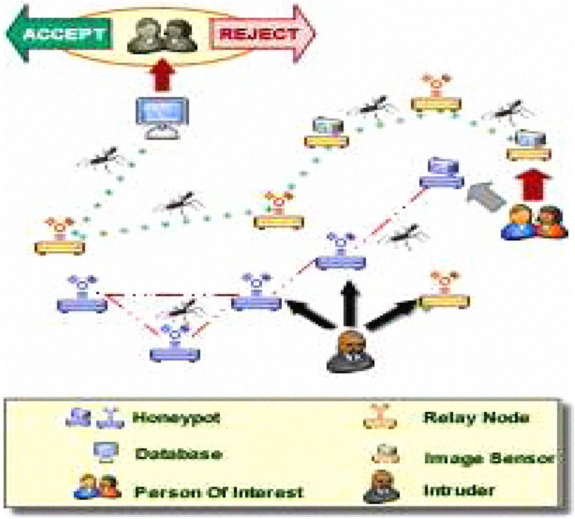


Fig. 2.Honeypot Framework implemented Using SI

IV. Conclusion

The simulation in this paper shows that for the battlefield monitoring application, CRP can make the packet delivery rate high and bit error rate depending on message prioritization. This proposed Honeypot using SI framework will be simulated using real-time environment to test robustness of the algorithm. This approach could promise a network free from attacks such as physical layer jamming attack, collision attack, and Worm-hole attacks in data-link layer etc. The convenience of tracking the intruder using Honeypot is based on cost, time, sensitivity and resource availability of the application.

V. References

[1] Kennedy J, Shi Y. and Eberhart R.C., "Swarm Intelligence", Morgan Kaufmann Publishers, San Francisco, 2001.

[2] A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks", IEEE Computer, Vol 35, Issue: 10, Oct 2002.

[3] Muraleedharan R and Osadciw L.A., "Security: Cross Layer Protocol in Wireless Sensor Network", INFOCOM 06, Barcelona, Spain, Apr 2006

[4] Muraleedharan R and Osadciw L.A., "Secure Health Monitoring Network Against Denial-Of-Service Attacks Using Cognitive Intelligence, CNSR, Halifax, Canada, pp 165-170, 2008.

[5] Provos N., "A Virtual Honeypot Framework", Technical Report 03-1. CITI, 2003

[6] Kreibich. C and Crowcroft M.C., "Honeycomb: Creating Intrusion Detection Signatures Using Honeypots", ACM SIGCOMM Computer Communication, pg 51-56, 2004.

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2009.7084
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2009.7084