Computer Communications 33 (2010) 619–638

Contents lists available at ScienceDirect

Computer Communications

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

Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks

Stefan K. Stafrace *, Nick Antonopoulos

Computing Department, School of Electronics and Physical Sciences, University of Surrey, Guildford, Surrey GU2 7XH, United Kingdom

ARTICLE INFO

Article history:
Received 21 January 2009
Received in revised form 18 September 2009
Accepted 6 November 2009
Available online 17 November 2009

Keywords:
Wireless ad hoc networks
Agent-based intrusion detection
Tactical agents
Military tactics
Security

ABSTRACT

Wireless Ad hoc Networks (WAHNs) offer a challenging environment for conventional Intrusion Detection Systems (IDSs). In particular WAHN have a dynamic topology, intermittent connectivity, resource constrained device nodes and possibly high node churn. Researchers over the past years have encouraged the use of agent-based IDS to overcome these challenges. In this work we propose the use of military tactics to optimise the operations of agent-based IDS for WAHN. We design an agent framework modeled over a military command structure and an agent behavioural model, which employs adapted military tactics to police routes, and detect intruders in the network. The tactical agents follow a risk-based approach such that the frequency of patrols is directly proportional to the risk factor of the route. Consequently, resources are conserved without impacting the effectiveness of the IDS. We demonstrate the proof of concept through a case study. In this study, we implement a simulation-based model of our solution to detect and recover from a Sinkhole attack in a Wireless Sensor Network (WSN), using the Ad hoc On Demand Distance Vector (AODV) as routing protocol. We evaluate the proof of concept in terms of the detection precision, data loss incurred from the attack and the agent overheads due to mobility and communication.

1. Introduction

A Wireless Ad hoc Network (WAHN) is an open network system consisting of autonomous nodes, which communicate in a peer-to-peer fashion over a wireless medium. The member nodes can join or leave the network on their own accord [4]. Each node acts both as a host and as a router; hence, communication between a source and a destination node is achieved through ad hoc multihop routing over the intermediate nodes. The characteristics of WAHNs pose new challenges to the traditional Intrusion Detection Systems (IDSs) used in wired network environments [5]. In particular, the dynamic network topology and the lack of an infrastructure does not allow for key elements of the IDS to be positioned in strategic locations within the network. Furthermore, the wireless channel is a shared medium that does not require for the participating devices to be physically attached to the network. In addition, some of the wireless devices could also be mobile. Consequently, whilst roaming around, the device might be physically captured and tampered by malicious adversaries. Therefore, it is more difficult to establish a concrete boundary for the IDS to operate within. Lastly, the design and operations of the IDS are affected by the resource constraints of some of the wireless devices, in particular, limited communication bandwidth, processing, storage and energy capacity.

It is evident from the above that alternate IDS designs had to be sought to overcome these challenges. Over the past decade, researchers have proposed agent-based IDS as a suitable distributed design approach to provide peer-to-peer intrusion detection and response capabilities to WAHN [4,5,8,25,26]. Jansen [6] defines a software agent as being a program that acts on the behalf of an entity, which could be either an individual or an organization. The agent is autonomous and has clear objectives to achieve. Agents can collaborate with each other and also interact with the hosting environment. In their survey on IDS, Kabiri and Ghorbani [8] describe the two main design paradigms in an agent-based approach. In the first design, agents are stationed in fixed positions all over the network. These agents can communicate amongst themselves and are used mainly for monitoring purposes. In the second design, mobile agents are deployed within the network. These types of agents can roam around the network, as required, to gather information and carry out other IDS operations. In the first approach the IDS agents have a better overall perspective of the network, but a higher traffic load due to communication overheads [8]; in the second approach, as explained by Jansen [6] and Hijazi and Nasser [5], the mobile agents provide added benefits to the system, in particular: reduced network traffic load and latency,

* Corresponding author. Tel.: +44 1483 68 2263.
E-mail addresses: s.stafrace@surrey.ac.uk, stefan.stafrace@gmail.com (S.K. Stafrace), n.antonopoulos@surrey.ac.uk (N. Antonopoulos).

0140-3664/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2009.11.006

bandwidth conservation and adaptation to dynamic topologies and heterogeneous networks. On the negative side, mobile agents have two main disadvantages. Firstly, the mobile agents themselves are considered as vulnerabilities that might be exploited to compromise the system and, secondly, the mobility overhead could add extra weight to the overall solution.

1.1. Research goals

In this paper, we propose a solution based on a hybrid of both design approaches mentioned previously, using a new breed of agents – *Tactical Agents*. We use the term *tactical* to describe agents that are used for policing and defensive maneuvers. The behavioral model of these agents is inspired by military operations and tactics. For centuries military tactics have been studied, evaluated and improved to yield efficient and effective standard operating procedures, which are in use by all major modern military organizations [13,23]. We research the possibility of adapting and applying this knowledge to the design of an agent-based IDS framework deployed on WAHN. The rationale for the use of tactical agents originated from visualizing the WAHN as an urban hostile zone, where the agents collaboratively follow specific tactics to police the zone. Similarly, in a real case scenario, military patrol squads systematically scout through various urban zones to determine whether there are adversaries disguised as civilians. The adversary is identified through behavior analysis and feature extraction. The patrol squad employs an efficient collaboration model to carry out their duties.

Our main focus in this piece of work is on the design of the agent-based framework and the behavioural model employed by the tactical agents. We are concerned with optimising the operations of an agent-based IDS in WAHN, by reproducing a similar degree of efficiency and effectiveness, which is exhibited in military organisations. We investigate the use of risk-based prioritization in deploying the tactical agents to avoid the unnecessary consumption of resources. A focal point in military tactics [23], such approach could be key in efficiently distributing resources to defend high and low risk routes. We describe routes as being high risk when they have a considerable high throughput and constant stability (i.e. frequency of use); hence, such route would potentially incur maximum damage in the presence of an intruder. We consider this work as an initial feasibility study on the potential use of tactical agents, with the ultimate goal of demonstrating the proof-of-concept through a case study. In this case study we test our proposed solution in a Wireless Sensor Network (WSN) simulator against the Sinkhole Attack on the Ad Hoc On Demand Distance Vector (AODV) routing protocol. We used WSN as part of our case study for demonstration purposes; nonetheless, we could have opted for a general wireless ad hoc network environment. Ultimately we evaluate the efficiency and effectiveness of the solution within the context of the test scenario by measuring the detection precision, the data packet loss due to the attack and the communication overheads in terms of messages exchanged. The long term goal of this work, which requires much further research, is for our proposed solution to eventually cater for a diverse range of known (and also unknown) attacks in distributed network environments.

The rest of the paper is organised as follows:

In Section 2, we provide some background information on various proposed solutions for agent-based intrusion detection systems in WAHN.

In Section 3, we focus on the three main components of our case study: Wireless Sensor Network (WSN), Sinkhole Attack and the AODV routing protocol. We provide an overview of WSN and describe the *modus operandi* of the Sinkhole Attack. Furthermore, we explain the workings of AODV.

In Sections 4 and 5, we present our proposed intrusion detection system based on tactical agents. We describe the requirements that the solution should satisfy in alignment with our research objective; the assumptions taken for our proof of concept; the design rationale of the agent framework and the implementation considerations for the simulation.

In Section 6, we discuss the metrics used to evaluate the proof of concept. We interpret the results of the experiments conducted through the simulation.

We conclude with Section 7 where we remark on what was actually achieved through this piece of work. We also highlight the future work that needs to be carried out to achieve the long term research goal.

2. Related work

We have considered various agent-based intrusion detection models that have been presented in the literature over the past years [15]. Through this analysis, we extracted the specific design characteristics of the architectures adopted by the examined models, and then related them accordingly to the concepts of a military structure and operation tactics. This exercise served also as an attempt at substantiating the military-inspired, design paradigm used in our proposed solution.

The design feature that is evident is the use of a hierarchy of agents to separate functionality. As explained in [1,9], this approach allows for scalability, the efficient use of resources and the restriction of computational-intensive activity to fewer nodes. Hierarchy and separation of duties are also two distinctive features of a military structure. AAFID [1] uses leaf agents to collect data within host nodes and transceiver agents to assimilate information from the collected data. The transceiver agents report their findings to monitor agents, which are responsible for the actual decision making. A monitor agent is associated with one or more transceiver agent. This could be viewed as a single point of failure. Consequently, a transceiver agent can report to one or more monitor agent to provide the necessary redundancy. The drawback is that a mechanism has to be in place to ensure that each listening monitor agent is informed accordingly, which naturally results in communication overheads.

Similarly in [12], the MA-IDS architecture employs a hierarchy of agents with specific roles, namely, Manager, Assistant Mobile Agent, Response Mobile Agent and Host Monitor agent. The Host Monitor agent is fixed on each host node and is responsible for the local intrusion detection. It reports directly to the Manager agent, which also resides on the host. If the Host Monitor agent cannot conclude decisively on whether an intrusion is happening, it resolves to the help of the Manager component. The latter dispatches an Assistant MA to patrol the neighbourhood on a specific itinerary. The agent collects intrusion detection-related information from the visited nodes. On its return back, the Manager uses the collected information to decide whether a distributed intrusion is in effect. If so, the Manager dispatches a Response MA to take the necessary action accordingly. The MA-IDS model introduces the concept of patrols, which also has a military connotation.

IDSA [21] and MAPIDS [25] move a step further to apply society inspired semantics to the hierarchical structure of the IDS. The advantage in mimicking social behaviour is to optimise the cooperation and communication amongst the agent community that make up the IDS. In an analogous manner, we apply military inspired semantics to achieve the same outcome, hopefully, with improved results. IDSA consists of a number of agents, more specifically, Chief, Detectives and Cops. It also introduces the concept of virtual neighbourhoods, which can be thought of as clusters of nodes. The cops are mobile agents that are dispatched by