Computer Communications 34 (2011) 468–484

Contents lists available at ScienceDirect

Computer Communications

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

Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks

Z.A. Baig *

Computer Engineering Department, King Fahd University of Petroleum & Minerals, P.O. Box 293, Dhahran 31261, Saudi Arabia

ARTICLE INFO

Article history:
Available online 13 April 2010

Keywords:
Wireless Sensor Networks (WSNs)
Node exhaustion
Malicious attacks
Pattern recognition
Distributed processing

ABSTRACT

Malicious attacks when launched by the adversary-class against sensor nodes of a wireless sensor network, can disrupt routine operations of the network. The mission-critical nature of these networks signifies the need to protect sensory resources against all such attacks. Distributed node exhaustion attacks are such attacks that may be launched by the adversarial class from multiple ends of a wireless sensor network against a set of target sensor nodes. The intention of such attacks is the exhaustion of the victim's limited energy resources. As a result of the attack, the incapacitated data-generating legitimate sensor nodes are replaced with malicious nodes that will involve in further malicious activity against sensory resources. One such activity is the generation of fictitious sensory data to misguide emergency response systems to mobilize unwanted contingency activity. In this paper, a model is proposed for such an attack based on network traffic flow. In addition, a distributed mechanism for detecting such attacks is also defined. Specific network topology-based patterns are defined to model normal network traffic flow, and to facilitate differentiation between legitimate traffic packets and anomalous attack traffic packets. The performance of the proposed attack detection scheme is evaluated through simulation experiments, in terms of the size of the sensor resource set required for participation in the detection process for achieving a desired level of attack detection accuracy. The results signify the need for distributed pattern recognition for detecting distributed node exhaustion attacks in a timely and accurate manner.

1. Introduction

Wireless sensor networks have emerged as a significant source of data collection based on sensing of the immediate environment of the sensor nodes. Sensor networks are deployed in harsh and inaccessible environments with the purpose of monitoring their respective surroundings, and generating observed readings, for delivery to a centralized entity, for further data analysis. Sensor nodes are tiny devices with limited available resources (power, processing and memory) for performing all their sensory operations, and be sustained for their entire lifetime. Applications of wireless sensor networks such as battlefield monitoring, bushfire monitoring and surveillance, are mission-critical in nature. The timeliness and accuracy in the delivery of the sensory data affects several contingency efforts that may be launched upon successful detection of a particular event in the environment. Therefore, it is essential to protect such networks from malicious attacks, that may be launched by the adversary-class, with the intent of causing loss to such networks.

The limited on-board memory resources of the sensor nodes restricts the size of applications, program codes and actual data that can be stored in their memory. The on-chip processing capability of the Berkeley Mica sensor [1], operating at 4 MHz, is several orders of magnitude less than that of a standard desktop processor. Sensor nodes are generally supplied with power from batteries (8 mW for a Mica sensor node). Program codes and applications that demand large numbers of CPU cycles for execution may exhaust the limited energy of the sensor node much earlier than the anticipated lifetime of the node. It is thus evident that most applications and programs designed for high-performance computing devices cannot be accommodated unaltered into the small memory space of sensor nodes. All applications and programs designed for such resource-constrained devices must be light-weighted and compact in nature.

Sensor nodes are prone to a plethora of possible malicious attacks that may be launched by the adversary-class from either within or outside the network. Deployment of sensor nodes over a larger geographical area makes them even more vulnerable to any of these attacks [2]. Distributed node exhaustion attacks are launched from multiple ends of a network towards a set of victim nodes, with the intent of exhausting their limited resources; exploiting the disparity which exists between the network

* Tel.: +966 3 860 7548; fax: +966 4 860 3059.
E-mail address: zbaig@kfupm.edu.sa

0140-3664/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2010.04.008

bandwidth and the target's limited resource availability. As a result, the victims are incapacitated from further participation in crucial network operations such as provisioning of service to legitimate clients [3–5].

In this paper, distributed node exhaustion attacks are defined as attacks launched by the adversary-class from multiple ends of the network with the intent of exhausting the limited energy resources of the victim nodes. As a result of the attack, access to sensory readings by the base station is denied. Due to the distributed nature of the attack, these attacks are analogous to Distributed Denial of Service attacks [3] in high performance computer networks. As a result of the attack, target nodes are overwhelmed with higher than normal intensities of traffic inflow, that will lead to the rapid exhaustion of their limited energy resources; incapacitating them from further participation in crucial network operations [2,6]. It is postulated that for timely and accurate detection of such attacks, predefined patterns of normal network traffic flow must be programmed in a conglomerate of collaborating sensors with attack detection capabilities.

In [7], we proposed a simple attack detection scheme to detect a class of distributed attacks, namely distributed denial of service, in wireless sensor networks. The scheme did not address the issue of the presence of adversaries with varying capabilities, and lacked the flexibility to detect attacks under varying network conditions. In contrast to the work done earlier, in this paper a robust adversary model for a distributed node exhaustion attack is formulated. In addition, a distributed pattern recognition scheme is defined to efficiently detect such an attack.

The contributions of this paper are listed as follows:

- An adversary (attack) model is proposed to define capability-based malicious nodes.
- An adversary node energy usage model is defined to signify the potential strength of the attack.
- A network model is defined to classify wireless sensor networks into three distinct data delivery models.
- A distributed, pattern recognition scheme for distributed node exhaustion attack detection in wireless sensor networks is defined.
- A detailed simulation analysis to test the effectiveness and performance of the proposed scheme is performed.

Throughout the rest of the article, the term *attack* has been used for referring to a *distributed node exhaustion attack*.

The paper is organized as follows: the background is given in Section 2. Section 3 defines the attack model for a distributed node exhaustion attack. The network model for a wireless sensor network is defined in Section 4. A pattern-based model for normal and anomalous network traffic is defined in Section 5. The attack detection scheme is given in Section 6. Section 7 describes the method used for generating optimal time frames, as a parameter, necessary for accuracy in the attack detection process. In Section 8, the algorithm for the selection of decision-making nodes for the attack detection scheme is defined. In Section 9, a qualitative analysis of the efficiency of the attack detection scheme is given. The results and analysis of the simulations are elaborated upon in Section 10. The concluding remarks are given in Section 11.

2. Background

Although several pattern recognition schemes for network intrusion detection have been proposed in the literature, their centralized nature, with intensive resource demands make them infeasible for deployment on sensor networks. It may be noted that schemes proposed for detecting distributed denial of service attacks can be modified to detect node exhaustion attacks in sensor networks. However, a detection scheme to explicitly detect such attacks in sensor networks does not exist. In [8], the authors propose a centralized neural network-based technique to detect DDoS attack patterns by means of processing of extracted traffic flow features on a centralized pattern recognition engine. In [9–11], Self-Organizing Maps (SOMs) have been used for anomaly intrusion detection in high-performance networks. SOM-based approaches impose a high demand on processing and memory resources, and are not inherently distributed in nature. A cooperative, distributed DDoS attack mitigation approach for high-performance networks has been proposed by [12]. In their scheme, individual nodes perform local detection of anomalous traffic, and subsequently rely on gossip information to share their observations, so as to achieve accuracy in packet dropping process.

A localization anomaly detection scheme for wireless sensor networks is proposed by [13] for detecting anomalies in the messages communicated by beacon nodes of the network. Sensors use static deployment knowledge to verify the location claims of other sensor nodes using one of several proposed metrics. Subsequently, the sensors rely on message broadcasts from peer sensor nodes to create local observation lists for comparison and verification purposes. [6] have classified DoS attacks at various layers of operation within a typical sensor network. They have also suggested ways to counter DoS attacks at the different layers. [14] defines DoS attacks in Mobile Ad Hoc networks as "sleep deprivation torture" or "battery exhaustion attacks". In such attacks, energy-constrained nodes are prevented from entering normal low power idle or sleep states during their cycles of operation, thus leading to the rapid exhaustion of their energy resources. [15] propose a mechanism for detecting denial of message attacks in sensor networks. In their scheme, selective nodes are sampled using controlled probabilistic checking to request acknowledgements for message broadcasts. Considering that adversaries are unaware of the selected nodes to be sampled at any given time, the scheme ensures that legitimate messages are not deliberately dropped as part of the attack. An approach for optimal placement of intrusion detection nodes in sensor networks has been proposed by [16]. In this scheme, the authors assume that all intrusion detector nodes are tamper resistant, and are therefore not compromisable.

In [17], the authors propose a counter measure against path-based denial-of-service (PDoS) attacks in sensor networks. In such attacks, adversaries inject a sequence of spurious packets along established routing paths of the network. One-way hash chains are used here to prevent the adversaries from generating an unused hash chain value, thus constraining the effects of the attack.

The openly exposed nature of wireless sensor networks, along with the limited energy resources available to individual sensor nodes imply minimization of the number of messages exchanged. In such environments, message communication between the sensor nodes based on frequent broadcasting for purposes of attack detection may not be the most efficient solution, and will lead to rapid exhaustion of the sensor energy resources. The lack of a single entry point to the network implies that such attacks need to be detected by a set of cooperating nodes operating in a distributed manner in the network. The observation and comparison of network traffic with known patterns of normal network behavior is an effective approach for detecting such attacks. It is therefore postulated that if patterns of known traffic flow in the network are pre-configured, and constantly updated in attack detector nodes, observations and comparisons can be made to detect anomalies in the traffic flow. For this purpose, it is proposed to extend the pattern recognition capabilities of an associative memory scheme, namely the Graph Neuron [18–20], to to facilitate the successful detection of distributed node exhaustion attacks in sensor networks. The proposed algorithm relies on the cooperative intelligence of the set of detector nodes, namely GN nodes, for attack detection purposes.