Engineering Science and Technology, an International Journal 19 (2016) 782–799

HOSTED BY

Contents lists available at ScienceDirect

Engineering Science and Technology, an International Journal

journal homepage: http://www.elsevier.com/locate/jestch

Full Length Article

Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation

Basant Subba, Santosh Biswas *, Sushanta Karmakar

Department of Computer Science & Engineering, Indian Institute of Technology, Guwahati, Assam 781039, India

ARTICLE INFO

Article history:
Received 14 April 2015
Received in revised form
4 November 2015
Accepted 4 November 2015
Available online 18 December 2015

Keywords:
Mobile Ad-hoc Network (MANET)
Intrusion detection system (IDS)
Game theory
Bayesian Nash equilibrium

ABSTRACT

Present Intrusion Detection Systems (IDSs) for MANETs require continuous monitoring which leads to rapid depletion of a node's battery life. To address this issue, we propose a new IDS scheme comprising a novel cluster leader election process and a hybrid IDS. The cluster leader election process uses the Vickrey–Clarke–Groves mechanism to elect the cluster leader which provides the intrusion detection service. The hybrid IDS comprises a threshold based lightweight module and a powerful anomaly based heavyweight module. Initially, only the lightweight module is activated. The decision to activate the heavyweight module is taken by modeling the intrusion detection process as an incomplete information non-cooperative game between the elected leader node and the potential malicious node. Simulation results show that the proposed scheme significantly reduces the IDS traffic and overall power consumption in addition to maintaining a high detection rate and accuracy.

1. Introduction

Mobile Ad-hoc Networks (MANETs) are a collection of heterogeneous, infrastructure less, self organizing and battery powered mobile nodes with different resources availability and computational capabilities. The dynamic and distributed nature of MANETs makes them suitable for deployment in extreme and volatile environmental conditions. They have found applications in diverse domains such as military operations, environmental monitoring, rescue operations etc. Each node in a MANET is equipped with a wireless transmitter and receiver, which enables it to communicate with other nodes within its wireless transmission range. However, due to limited wireless communication range and node mobility, nodes in MANET must cooperate with each other to provide networking services among themselves. Therefore, each node in a MANET acts both as a host and a router.

The dynamic and distributed nature of MANETs make them vulnerable to various types of attacks like black hole attack, traffic distortion, IP spoofing, DoS attack etc. Malicious nodes can launch attacks against other normal nodes and deteriorate the overall performance of the entire network [1–3]. Unlike in wired networks, there are no fixed checkpoints like router and switches in MANETs, where the Intrusion Detection System (IDS) can be deployed [4,5]. Therefore, nodes in MANETs must cooperate in many aspects including intrusion detection for their well being [6–8]. IDSs have been deployed with great degree of success across diverse domains like wireless Ad-hoc networks [5,9], MANETs [10–12], wireless sensor networks [13], cyber-physical system [14], cloud computing [15], large scale complex critical infrastructures [16] etc. In this paper, we focus on IDS for MANETs.

Due to absence of any centralized monitoring entity in MANETs, each node runs its own IDS and usually operates in a promiscuous mode. However, owing to limited battery life, it is not feasible to keep the IDS running continuously on MANET nodes. Most of the current MANET IDS schemes do not take into account the nature of the environment they are operating in and therefore they end up monitoring all nodes with equal probability, irrespective of whether or not the node being monitored has a history profile of being malicious. This results in a poor monitoring strategy wherein the node operating the IDS ends up wasting most of its energy monitoring the normal nodes. Another issue with many MANET IDS schemes [17–19] is that they generate heavy intrusion detection related traffic. Unlike the wired networks, MANETs have limited bandwidth and therefore, a large amount of intrusion detection related traffic can cause severe congestion in the network and limit the flow of normal traffic. In addition, heavy intrusion detection traffic also leads to more energy consumption among MANET nodes for processing them.

Designing a MANET IDS scheme that is energy efficient and generates a low IDS traffic, while at the same time maintaining a high accuracy and detection rate is an active area of research. In this paper, we model the intrusion detection process in MANETs using a game theoretical framework. Game theory based MANET IDSs [20–22] have been found to be energy efficient as well as generate low IDS traffic

* Corresponding author. Tel.: +91 9957561026, +91-361-2583000.
E-mail address: santosh_biswas@iitg.ernet.in (S. Biswas).
Peer review under responsibility of Karabuk University.

http://dx.doi.org/10.1016/j.jestch.2015.11.001

through application of dynamic and economical monitoring strategies. Game theory based IDS models the intrusion detection problem as a non-cooperative game between two competing players (attacker and defender), where the defender player (cluster leader node) tries to maximize its payoff by increasing its probability of successful intrusion detection while the attacker player (malicious node) tries to minimize its probability of being detected by the IDS.

Game theory based IDS scheme allows the IDS to assess the type of the node being monitored and adopt appropriate monitoring strategies. Nodes are assigned maliciousness values based on the history profile of their observed actions. Unlike most conventional IDSs that adopt promiscuous monitoring strategy and results in high IDS traffic generation, game theory based IDS uses a dynamic monitoring strategy wherein nodes with high maliciousness values are monitored more frequently compared to nodes with low maliciousness values. This helps the IDS to conserve its energy and minimize the overall IDS traffic generation. In a game theoretic IDS framework, a rigorous monitoring strategy is adopted by the IDS if the environment it is operating in is hostile. On the other hand, if the environment is less hostile, a less rigorous monitoring strategy is adopted by the IDS.

Most of the game theory based IDSs proposed in the literature [19–21,23] assume a complete information game, wherein all players (nodes) have complete information about the game, i.e., they make an implicit assumption that various network parameters like energy levels and types of network nodes (normal or malicious), accuracy and detection rate of IDS etc. are known to all nodes *a priori*. But, such assumptions have limitations, since in most of the real network settings each node only has a limited information about the network parameters. Therefore, to address this issue of incomplete information game, we propose a Bayesian game theory based MANET IDS scheme that models the interaction between the attacker (malicious node) and the defender (node operating IDS) in MANET as a two person multi-stage, non-cooperative and incomplete information game. The Bayesian model [19] allows the node operating the IDS to adopt the most efficient monitoring strategy in an incomplete information game settings by examining the maliciousness history profile of the node being monitored and by evaluating the Bayesian Nash equilibrium of the game.

In summary, this paper proposes a MANET IDS scheme with the following objectives:

1. Modeling the intrusion detection process in MANETs as an incomplete information Bayesian game as nodes in MANETs only have partial information about the network.
2. Minimization of power consumption for operating IDS in MANETs.
3. Minimization of intrusion detection related traffic in MANETs.
4. Developing a MANET IDS scheme with high accuracy and detection rate.

To achieve these objectives, we propose a new MANET IDS scheme consisting of the following two components:

1. *A MANET leader election mechanism*: This component elects the cluster leader node using the VCG mechanism [24] and entrusts it with the responsibility of providing intrusion detection services to all other cluster nodes for a predefined period of time. Cluster leader elections are held at regular intervals which ensures uniform energy consumption among various cluster nodes for operating the IDS.
2. *A hybrid MANET IDS*: This component comprises one lightweight module and one heavyweight module. The lightweight module is less powerful but requires less energy for its operation. On the other hand, the heavyweight module is more powerful than the lightweight module but requires more energy for its operation. Initially only the lightweight module is activated. If the action of the node being monitored by the lightweight module is determined to be malicious then the heavyweight module is activated, else the decision to activate the heavyweight module is determined by the Nash Equilibrium of the non-cooperative game played between the elected leader node and the node being monitored.

The elected leader node operates the *hybrid MANET IDS*. Initially, only the lightweight module of the hybrid MANET IDS is activated, which calculates the Packet Forwarding Rate (PFR) of the potential malicious node being monitored. The PFR of any given node is defined as the ratio of total number of packets received to the total number of packets forwarded by the node over a given period of time. If the PFR of the node being monitored is less than the threshold value, then its action is assumed to be malicious and the heavyweight module is activated for more rigorous analysis. However, if the action of the node is found to be normal then the decision to activate the heavyweight module is determined by modeling the intrusion detection process as a multi-stage Bayesian game between two competing players, where the players of the game are the cluster leader node and the potential malicious node.

The cluster leader node has incomplete information about the type of the opponent node (normal or malicious) and the following two strategies: *Monitor* and *Not Monitor*. Here, the strategy *Monitor* corresponds to the activation of the heavyweight module. Similarly, the attacker player has two strategies: *Attack* and *Not Attack*. The Bayesian Nash Equilibrium (BNE) of the game is the strategy pair of the players which corresponds to the probability of the leader node to play its strategy *Monitor*/*Not Monitor* and the probability of the attacker player to play its strategy *Attack*/*Not Attack*. Intrusion detection process in MANETs is usually an incomplete information game, where nodes only have partial information about network parameters. The Bayesian game model allows the cluster leader node to formulate its monitoring strategies based on its belief about the type of the node (malicious or normal) being monitored without requiring a complete information about that node. It also minimizes the overall IDS traffic by adopting a non-promiscuous monitoring strategy.

Simulation results in NS-2 [25] show that the proposed MANET IDS scheme significantly reduces the power consumption for operating the IDS among MANET nodes by 15–20% compared to a random model. Further, the proposed scheme also maintains a high level of detection rate against *route compromise*, *traffic distortion* and *black-hole* attacks without introducing any significant traffic.

The rest of the paper has been structured in the following way. Section 2 discusses about the background and related works on intrusion detection in MANETs. Section 3 presents the overall description of our proposed MANET IDS scheme. Bayesian Game model used for developing energy efficient IDS monitoring strategies is discussed in section 3.1. A distributed and energy efficient MANET leader election mechanism is discussed in section 3.2. A hybrid MANET IDS along with its main components are discussed in section 3.3. Experimental results and performance evaluation of the proposed hybrid MANET IDS and MANET leader election mechanism are provided in Section 4. Finally, Section 5 provides the conclusion and future work.

2. Background and related works

In this section, we provide a brief background study on different types of MANET IDS based on their detection mechanism and modes of operation. We then discuss about various intrusion detection issues in MANETs and analyze the related works which have been categorized into non-game theory based and game theory based. Finally, the drawbacks associated with the related works have