Microprocessors and Microsystems 79 (2020) 103278

Contents lists available at ScienceDirect

Microprocessors and Microsystems

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

DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks

M. Premkumar [a,*], T.V.P. Sundararajan [b]

[a] Department of ECE, SSM Institute of Engineering and Technology, Dindigul, India
[b] Department of ECE, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India

ARTICLE INFO

Keywords:
Attack detection
Cluster-based key management
Countermeasures
Deep learning
Wireless sensor networks

ABSTRACT

Wireless Sensor Networks (WSNs) include small battery-based self-governing devices that are deployed in a distributed manner to supervise the environmental or physical circumstances. The routers and gateways are connected to the deployed nodes to support many real-time applications. Due to open access, the security issue arises in WSN. In this circumstance, the external users can be verified by securing authentication is necessary one. In real-time applications, to achieve secured communication they have made many lightweight authentication mechanisms. But WSNs are highly susceptible to DoS attacks as it lacks the synchronization between nodes during data routing. In this paper, a new lightweight DoS detection scheme Deep Learning-based Defense Mechanism (DLDM) has proposed to detect and isolate the attacks in Data Forwarding Phase (DFP). This paper describes the new algorithm for the successful detection of DoS attacks, such as exhaustion, jamming, homing, and flooding. We conduct extensive simulation experiments that can accurately isolate the adversaries and it is more resilient to DoS attacks. Our proposed simulation result shows that it can achieve a high detection rate, throughput, packet delivery ratio, and accuracy. This also reduces the energy consumption and the false alarm rate.

1.

In recent times, the Wireless Sensor Networks (WSNs) have introduced the broad series of applications and serves a major role in the current research domain. Information technology was developed; it recently became a primary component of the Internet of Things (IoT) [4, 26,37] . The WSNs spatially includes distributed small-sized low power sensor devices with the wireless radio transceiver to sense the various physical phenomena and collect the data in all types of environments. The WSNs could adapt to an extreme environment when the other wired and wireless networks (e.g. WLAN) are compared. The collection of data and establishing communication between one of the sink nodes of the base stations are involved [1,36,41]. So they are widely used in many civilian applications but are not limited to: the wild habitat monitoring [5], forest fire detection, real-time industrial monitoring and automation [3], building safety monitoring, traffic surveillance and control [2], constant health monitoring [6], military surveillance [7] and so on.

Due to their limited capabilities, random deployment, and unattended operations, the sensor nodes are liable to a different attack and having their security compromised in a severe environment like adversary areas [8,32]. During the deployment of WSN in the hostile region in which the sensor nodes are physically captured and manipulated, WSNs are particularly susceptible to DoS Attacks [9,33].

The network's capacity is diminished or eliminated and the termination of the usual communications by flooding a network with mass "useless" information is depleted by Denial of Services Attacks (DoS) [29]. DoS attacks in WSNs are generally different when compared with other wired and wireless networks. Almost every layer in WSNs is exposed to the variety of DoS attacks and it has varied attack techniques [9] which is illustrated in Table 1. There are many concepts developed to maintain the network from a DoS attack. A taxonomic analysis of wireless network jamming threats, how the DoS attacks targeting the different OSI layers of the WSN and their defensive strategies as described in [19].

The misbehaving nodes are usually identified by Watchdog based schemes and path rater is used to reroute without malicious nodes [11]. In the Reputation Rating scheme [12], the selfish nodes can be identified according to the function of neighbors of a single node such as energy consumption and packet forwarding.

The localization in WSN is achieved by Beacon-based algorithms or

* Corresponding author.
E-mail addresses: prem53kumar@gmail.com (M. Premkumar), suntvp@yahoo.co.in (T.V.P. Sundararajan).

https://doi.org/10.1016/j.micpro.2020.103278
Received 7 August 2020; Received in revised form 12 September 2020; Accepted 21 September 2020
Available online 25 September 2020

SSM Institute of Engineering and Technology DINDIGUL

Dr.D.SENTHIL KUMARAN, M.E., Ph.D., (NUS)
Principal
SSM Institute of Engineering and Technology
Kuttathupatti Village, Sindalagundu (Po),
Palani Road, Dindigul - 624 002.