Accepted Manuscript

A cognitive chronometry strategy associated with a revised cloud model to deal with the dishonest recommendations attacks in wireless sensor networks

Farah Khedim, Nabila Labraoui, Ado Adamou Abba Ari

PII: S1084-8045(18)30288-1
DOI: 10.1016/j.jnca.2018.09.001
Reference: YJNCA 2201

To appear in: *Journal of Network and Computer Applications*

Received Date: 22 September 2017
Revised Date: 4 June 2018
Accepted Date: 4 September 2018

Please cite this article as: Khedim, F., Labraoui, N., Abba Ari, A.A., A cognitive chronometry strategy associated with a revised cloud model to deal with the dishonest recommendations attacks in wireless sensor networks, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2018.09.001.

A cognitive chronometry strategy associated with a revised cloud model to deal with the dishonest recommendations attacks in wireless sensor networks

Farah Khedim[a,*], Nabila Labraoui[a], Ado Adamou Abba Ari[b,c]

[a] *STIC, University of Tlemcen, Algeria*
[b] *LaRI, University of Maroua, Cameroon*
[c] *LI-PaRAD, Université Paris Saclay, University of Versailles Saint-Quentin-en-Yvelines, France*

Abstract

Wireless sensor networks (WSNs) face many security issues. When external attacks can be prevented with traditional cryptographic mechanisms; internal attacks remain difficult to be eliminated. Trust and reputation have been recently suggested by many researches as a powerful tool for guaranteeing an effective security mechanism. They enable the detection and the isolation of both faulty and malicious nodes. Nevertheless, these systems are vulnerable to deliberate false or unfair testimonies especially in the case of dishonest recommendations attacks, i.e. badmouthing, ballot-stuffing and collusion attacks. In this paper, we propose a novel bio inspired trust model for WSNs namely Bee-Trust Scheme (BTS) based on the use of both a modified cloud model and a cognitive chronometry parameter. The objective of the scheme is to achieve both a higher detection rate and a lower false positive rate of dishonest recommendations attacks by allowing the distinction between erroneous recommendations and dishonest ones which has thus far been overlooked by most research work. Simulation results demonstrate that the proposed scheme is both effective and lightweight even when the number of dishonest recommenders is large.

Keywords: Trust and reputation systems, Security, WSN, Bad mouthing, Ballot stuffing, Cloud model, ABC

1. Introduction

1.1. Background

Over the past few years, wireless sensor networks (WSNs) have proven to be one of the most useful technologies due to the fact that they are potentially low-cost solutions to a variety of real-world challenges [1]. The continuous development of WSNs has contributed to their extensive application in various industries, including in key areas such as the electrical, healthcare, and military industries [2]. However, as for all technologies, the advantages of WSNs are often diminished due to the presence of risk factors and potential for abuse [3]. The capture of a sensor node will reveal all the security mechanisms as well as all network information to the adversary which can easily generate the so-called insider attacks, bypassing encryption and password security systems [4]. As a result, the adversary node may be taken as normal one in the network, which makes it possible to delete, intercept, or insert wrong information and can successfully pass the authentication process with their neighbors. Once a node is compromised, the integrity and availability of the entire network applications can be destroyed [5]. Thus, network security is an absolute necessity in order to guarantee the proper functioning of the whole network. When asymmetry cryptographic protection deals with external attacks, internal attacks remain undetected. This situation leads to develop effective schemes that can cope with these attacks [6].

Trust and reputation model has recently been suggested as an effective and challenging issue in the security of wireless sensor networks [7]. Trust management is fundamental to identify malicious, selfish and compromised nodes which have been authenticated [8]. While many secure schemes focus on preventing attackers from entering the network through secure key management, trust management, on the other hand, takes a further step to protect the entire network even if malicious nodes have had access to it. This feature is achieved in order to complement cryptography and to promote a healthy collaboration relationship among participant sensors in WSNs [9].

Currently, the most effective way to defend internal attack is trust management system [10]. However, the performance of reputation models faces with several security issues that have not yet been solved completely. One type of these attacks is the dishonest recommendations attacks. A malicious node participating in reputation system can falsely accuse well-behaving nodes of malicious actions and give them untrustworthy feedback in order to lower or destroy their reputation (bad mouthing attacks) [6, 11]. Malicious nodes can also falsely increase their own reputation or give a higher recommendation for the other malicious nodes (ballot-stuffing attacks), compromising the network with the hope to change the outcome of a reputation vote to their advantage [12]. Several malicious nodes may also collaborate in order to cause greater harm to the network (collusion attack).

Dealing with dishonest recommendations attacks is a signif-

[*] Corresponding author
Email address: farahbouhamed@gmail.com (Farah Khedim)