A Trust Model for Detecting Device Attacks in Mobile Ad Hoc Ambient Home Network

Article · April 2016

DOI: 10.4018/IJAPUC.2016040102

Solomon A Akinboro
Bells University of Technology, Ota, Ogun State
19 PUBLICATIONS 10 CITATIONS
SEE PROFILE

Emmanuel Olajubu
Obafemi Awolowo University
31 PUBLICATIONS 38 CITATIONS
SEE PROFILE

International Journal of Advanced Pervasive and Ubiquitous Computing
Volume 8 • Issue 2 • April-June 2016

A Trust Model for Detecting Device Attacks in Mobile Ad Hoc Ambient Home Network

Akinboro Solomon, Department of Computer Science and Technology, Bells University of Technology, Ota, Nigeria

Emmanuel Olajubu, Department of Computer Science and Engineering, Obafemi Awolowo University, Ile Ife, Nigeria

Ibrahim Ogundoyin, Department of Information and Communications Technology, Osun State University, Osogbo, Nigeria

Ganiyu Aderounmu, Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria

ABSTRACT

This study designed, simulated and evaluated the performance of a conceptual framework for ambient ad hoc home network. This was with a view to detecting malicious nodes and securing the home devices against attacks. The proposed framework, called mobile ambient social trust consists of mobile devices and mobile ad hoc network as communication channel. The trust model for the device attacks is Adaptive Neuro Fuzzy (ANF) that considered global reputation of the direct and indirect communication of home devices and remote devices. The model was simulated using Matlab 7.0. In the simulation, NSL-KDD dataset was used as input packets, the artificial neural network for packet classification and ANF system for the global trust computation. The proposed model was benchmarked with an existing Eigen Trust (ET) model using detection accuracy and convergence time as performance metrics. The simulation results using the above parameters revealed a better performance of the ANF over ET model. The framework will secure the home network against unforeseen network disruption and node misbehavior.

KEYWORDS

Ad Hoc Home Network, Adaptive Neuro Fuzzy, Ambient, Device Attacks, Trust Management

1. INTRODUCTION

As the Internet's popularity grows, distributed applications are becoming important. The rapid development of network and communication technologies metamorphose into new forms of distributed systems such as peer to peer (P2P) networks and mobile ad hoc networks (MANET) (Li and Singhal, 2007). MANET is a collection of autonomous nodes that communicate with each other by forming a multi-hop radio network and maintain connectivity in a decentralized manner (Zheng et al., 2003). Each node functions as both a host and a router. All members in the MANET equally participate in the routing information distribution and maintenance by running the same routing protocol.

Ambient intelligence (AmI) joins together the fields of ubiquitous computing and communications, context awareness and intelligent user interfaces. AmI is the capability of an environment populated by electronic devices to exhibit a certain degree of intelligence. To be perceived as intelligent, the whole

DOI: 10.4018/IJAPUC.2016040102

environment must act in a smart way and this requires that each component in the environment actively coordinates with others and at the same time, is supervised by the remaining environment (Giacomo et al. 2005). Within the context of AmI, MANET is likely to play major roles in which people are surrounded and supported by small context-aware, cooperative and non-obstructive devices that will aid our everyday life (Anna, 2012). The technologies used to deploy AmI are ubiquitous computing, ubiquitous communication and intelligent user interface. The ubiquitous computing will integrate microprocessors into the devices, ubiquitous communication enables these devices to communicate with each other by means of ad hoc or wireless networking and intelligent user interface allow the inhabitant of the AmI environment to control and interact with the environment in a natural and personalized way (Mariano and Beattriz, 2005).

An AmI environment that uses MANET will automatically connect devices that are equipped with short range communication medium based on their profiles, context such as location and social behavior (Juan and Qingrui, 2011) and this make the home devices to be prone to attacks. Attacks in AmI home can be on the communication channels or individual devices for examples battery power exhaustion and side channel attacks (Ingrid et al. 2005).

The energy exhaustion attacks are real threat without sufficient security because malicious node could prohibit another node to go back to sleep causing the battery to be drained. Side channel attacks occur when nodes are observed while in operation and the timing, power or electromagnetic variation are measured. This leakage of information through the side channel is a consequence of the energy dependency of the calculation on the data.

The attackers are very creative and always introduce novel attacks to the system. It is important to develop an intrusion detection system (IDS) that will detect such attack packets before it wreck havoc to the life in the ambient home. An IDS is expected to detect previously known attacks with high accuracy, detect previously unseen attacks to minimize the losses as a result of a successful intrusions and also detect attacks at an early stage to minimize their impact.

Because users of MANET do not have previous interactions, it is more important to establish an acceptable level of trust relationships among participating users as a means of detecting malicious nodes and securing home devices. Trust is defined as a set of relations among entities that participate in a protocol. These relations are based on the evidence generated by the previous interactions of entities within a protocol. In general, if the interactions have been faithful to the protocol, then trust will accumulate between these entities (Eschenauer *et al.*, 2002).

In this research work, emphasis is on how to detect malicious nodes as a means of securing the AmI home devices and appliances against attacks. A model called global reputation aggregation that considered the direct and indirect communication of home and remote devices was developed for the security system. This model establishes certain level of trust before a new or existing user device can be allowed to interact with the home.

The rest of the paper is organized as follows: review of related literature is presented in section 2. Presented in section 3 are conceptual framework for the proposed ambient home network, description of the proposed model and algorithms. Section 4 presented simulation results and discussion, while conclusion is in section 5.

2. REVIEW OF RELATED LITERATURE

The review of existing trust models was done to identify the system approaches adopted. Juan and Qingrui (2011) proposed mobile trust model, a spontaneous mobile social network that was fully decentralized and self-managed using experienced user, inexperienced user, similarities of user profile,