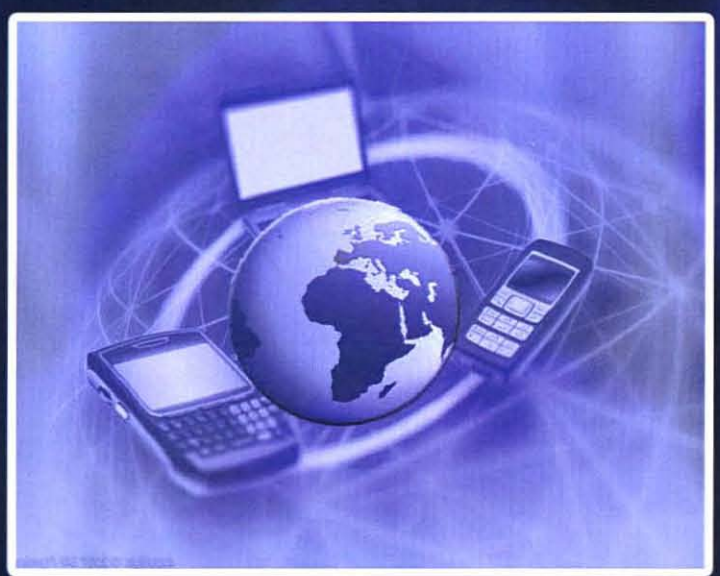
Research Issues in Wireless

Communications and Networking

Farhat Anwar
Wajdi Al-Khateeb



IIUM Press
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

Research Issues in Wireless Communications Networking

Farhat Anwar & Wajdi Al-Khateeb

IIUM Press

Published by:
IIUM Press
International Islamic University Malaysia

First Edition, 2011

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Farhat Anwar & Wajdi Al-Khateeb: Research Issues in Wireless Communications Networking

ISBN: 978-967-418-149-9

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN.BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan
Tel: +6**03-6188 1542 / 44 / 45** Fax: +6**03-6188 1543**
EMAIL: iiumprinting@yahoo.com

CHAPTER 34

INVESTIGATION OF TECHNIQUES FOR COMBATING MALICIOUS OBJECTS IN UNRELIABLE WIRELESS SENSOR NETWORKS

Abdulazeez F. Salami[1,a], Habeeb Bello-Salau[2,b], Muktar Hussaini[3,c], Farhat Anwar[4,d]
[1,2,3,4]ECE Dept, Fac. of Eng., International Islamic Univ. Malaysia (IIUM)
Jalan Gombak, 53100 Kuala Lumpur, Malaysia
[a]kermkerm1@gmail.com, [b]bellosalau@gmail.com, [c]intaiium@gmail.com, [d]farhat@iium.edu.my

34.1 INTRODUCTION

Unreliable networks can take many different forms such as in the general case an ad hoc network or more specifically as a wireless sensor networks (WSNs). Some of the fields you can find these types of networks used in would be the telecommunications industry with mobile phones, biological research for monitoring animals in the wild and military applications to monitor soldiers. Networks in these areas are handling an increasing amount of data. This data is very valuable and therefore a source of concern in making sure that none of it is lost or damaged. From a security standpoint there are many ways that an attack on these types of networks can be implemented. Some attacks are rather difficult to execute and would require knowledge of the particular network that is being attacked to be effective. One of the most effective attack methods would be for the attacker to inject its own data into the network either with the simplest goal of consuming network resources or having some other purpose such as capturing or corrupting the data stored in the network. Thinking in terms of biological systems the data that these attackers inject into the network is similar to a virus entering a human body. In the medical field medicine can be used to help cure a person by targeting this virus, in much the same way this chapter considers introducing a special type of anti-virus to the network to remove this data inserted by an attacker. This chapter considers leveraging the properties of unreliable network combined with a recommended approach employing an anti-virus to remove the virus from the network effectively [1, 2].

34.2 PRÉCIS OF FUNDAMENTAL CONCEPTS

34.2.1 Unreliable Networks

One can picture an unreliable network as an undirected graph. What makes this network unreliable is that none of the edges between nodes is guaranteed. Figure 34.1 shows an example of an undirected graph. In terms of a wireless sensor network you can think of the lines between the nodes as wireless connections [2]. Looking at nodes (a), (b), (e) in the figure you can see that (a) is connected to (e) by (b). If (b) were to die then (a) and (e) would have no path for communication between the two. In wireless networks it is said that the link between the two nodes is down by either one node being dead or if there is just problems in communication between these nodes. This means that the layout and paths through this network are always changing. In some cases two parts of the network may be unable to communicate with each other [3].