1. Record Nr. UNINA9910452741903321

Titolo	Fatigue crack growth [[electronic resource]] : mechanics, behavior and prediction / / Alphonse F. Lignelli, editor
Pubbl/distr/stampa	New York, : Nova Science Publishers, c2009
ISBN	1-60876-770-1
Descrizione fisica	1 online resource (278 p.)
Altri autori (Persone)	LignelliAlphonse F
Disciplina	620.1/126
Soggetti	Materials - Fatigue Fracture mechanics Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.

2. Record Nr. UNISA996426331803316

Autore	Fazeldehkordi Elahe
Titolo	A study of black hole attack solutions : on AODV routing protocol in MANET / / Elahe Fazeldehkordi, Iraj Sadegh Amiri, Oluwatobi Ayodeji Akanbi, University of Malaya, Kuala Lumpur, Malaysia ; Matthew Neely, technical editor
Pubbl/distr/stampa	Waltham, MA : , : Elsevier, , [2016] ©2016
ISBN	0-12-805367-4 0-12-805379-8
Edizione	[1st edition]
Descrizione fisica	1 online resource (124 p.)
Collana	Syngress advanced topics in information security
Soggetti	Ad hoc networks (Computer networks) Routing protocols (Computer network protocols) Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Front Cover; A Study of Black Hole Attack Solutions; Copyright Page; Contents; List of Tables; List of Figures; Preface; 1 Introduction; 1.1 Introduction; 1.2 Problem Background; 1.3 Problem Statement; 1.4 Intent of Study; 1.5 Aims; 1.6 Scope; 1.7 The Significance of the Book; 1.8 Organization of the Book; 2 Literature Review; 2.1 Introduction; 2.2 Network; 2.3 Wired Networks; 2.4 Why Wireless Networks?; 2.5 Wireless Networks; 2.5.1 IEEE Standard for Wireless Networks; 2.5.2 Categorization of Wireless Networks; 2.5.2.1 Infrastructure Networks; 2.5.2.2 Infrastructure-Less Networks 2.5.3 Benefits of Wireless Networks2.5.4 Weaknesses of Wireless Networks; 2.6 Ad Hoc Networks; 2.6.1 Static Ad Hoc Networks; 2.6.2 Mobile Ad Hoc Networks (MANETs); 2.6.2.1 Categorization of MANETs; 2.6.2.1.1 Vehicular Ad hoc Networks (VANETs); 2.6.2.1.2 Intelligent Vehicular Ad hoc Networks (InVANETs); 2.6.2.1.3 Internet-Based MANETs (IMANETs); 2.6.2.2 Features of MANET; 2.6.2.3 Utilization of MANET; 2.6.2.4 Benefits of MANET; 2.6.2.5 Weaknesses of MANET; 2.7 Routing; 2.8 Ad Hoc Network Routing Protocols; 2.9 MANETs Routing

Protocols; 2.9.1 Categorization of Routing Protocols
2.9.1.1 Table-Driven (Proactive) Routing2.9.1.2 Reactive (On-Demand) Routing; 2.9.1.3 Hybrid Routing; 2.10 Optimized Link State Routing Protocol (OLSR); 2.10.1 OLSR Working; 2.10.1.1 Multipoint Relaying (MPR); 2.11 Ad Hoc on Demand Distance Vector Routing Protocol (AODV); 2.11.1 Routing in AODV; 2.11.1.1 Route Discovery Mechanism in AODV; 2.11.1.2 Route Maintenance Mechanism in AODV; 2.11.2 Features of AODV; 2.11.3 Benefits and Weaknesses of AODV; 2.12 Dynamic Source Routing Protocol (DSR); 2.12.1 Route Discovery Process; 2.12.2 Route Maintenance Process; 2.13 Security Challenges in MANETs
2.13.1 Categorizations of MANET Attacks2.13.2 Black Hole Attack in MANETs; 2.13.3 Black Hole Attack in AODV; 2.13.4 Black Hole Attack in OLSR; 2.13.5 Other Attacks in MANETs; 2.13.5.1 Gray Hole Attack; 2.13.5.2 Flooding Attack; 2.13.5.3 Selfish Node; 2.13.5.4 Wormhole Attack; 2.13.5.5 Sleep Deprivation Torture Attack; 2.13.5.6 Jellyfish Attack; 2.13.5.7 Modification Attack; 2.13.5.8 Misrouting Attack; 2.13.5.9 Impersonation Attack; 2.13.5.10 Routing Table Overflow Attack; 2.14 Related Studies; 2.15 Investigated Solutions; 2.16 Intrusion Detection System (IDSAODV); 2.17 Evaluation Metrics
2.18 Summary3 Research Methodology; 3.1 Introduction; 3.2 Research Structure; 3.2.1 Phase 1: Investigating the Existing Solutions; 3.2.2 Phase 2; 3.2.2.1 Phase 2a: Clarifying Efficient Solution; 3.2.2.2 Phase 2b: Executing the Existed Solution; 3.2.2.2.1 Simulation: The Customary Definition; 3.2.2.2.2 Network Simulator (NS); 3.2.2.2.3 Tool Command Language (Tcl) in NS; 3.2.3 Phase 3: Comparing the Effects of Recommended Solution on MANET Performance; 3.3 Summary; 4 Investigation and Selection Procedure; 4.1 Introduction
4.2 Executing a New Routing Protocol in NS to Simulate Black Hole Behavior

Sommario/riassunto

Mobile Ad Hoc Networks (MANETs) are a popular form of network for data transfer due to the fact that they are dynamic, require no fixed infrastructure, and are scalable. However, MANETs are particularly susceptible to several different types of widely perpetrated cyberattack. One of the most common hacks aimed at MANETs is the Black Hole attack, in which a particular node within the network displays itself as having the shortest path for the node whose packets it wants to intercept. Once the packets are drawn to the Black Hole, they are then dropped instead of relayed, and the communication of the MANET is thereby disrupted, without knowledge of the other nodes in the network. Due to the sophistication of the Black Hole attack, there has been a lot of research conducted on how to detect it and prevent it. The authors of this short format title provide their research results on providing an effective solution to Black Hole attacks, including introduction of new MANET routing protocols that can be implemented in order to improve detection accuracy and network parameters such as total dropped packets, end-to-end delay, packet delivery ratio, and routing request overhead. Elaborates on the basics of wireless networks, MANETs Explains the significance behind the need of wireless networks and MANET security Understand MANET routing protocols, namely the ADOV method