



People's Democratic Republic of Algeria
Ministry of Highly Education and Scientific Research



Order N°:

M'SILA University
FACULTY OF Mathematics and Computer Science
Information Communication Sciences and technology Department

Dissertation
Dissertation Submitted in Partial Fulfillment of the Requirements for
MASTER degree
Domain: Mathematics and Computer Science
Branch: Computer Science
Specialty: Information Communication Sciences and technology

SUBJECT

**Security of Adhoc Networks Against Routing Protocols
Attacks**

Prepared by:
Benazzi Moussaab

Supervised by:
Benouis Mohamed

Promotion : 2014 /2015

Table of Contents

General introduction	1
Chapter 01 : Protocols and Communication Architectures	
1. Introduction.....	2
2. Notions about computer networks.....	2
2.1. Characteristics of networks	2
2.2. Classification of networks.....	2
2.2.1. Wireless Personal Area Networks (WPAN).....	3
2.2.2. Wireless Local Area Network (WLAN).....	4
2.2.3. Wireless Metropolitan Area Networks (WMAN).....	6
2.2.4. Wireless Wide Area Networks (WWAN).....	7
2.3. The network topologies.....	9
2.3.1. Bus Topology.....	9
2.3.2. Star Topology.....	9
2.3.3. Ring Topology.....	10
2.3.4. Mesh Topology.....	11
3. Normalization of the communication architecture.....	11
3.1. ISO/OSI Reference Model.....	11
3.1.1. The function of the OSI reference model:.....	11
3.1.2. The functions of each layer.....	12
3.1.2.1. Layer 7: The Application Layer.....	12
3.1.2.2. Layer 6: The Presentation Layer.....	13
3.1.2.3. Layer 5: The Session Layer.....	13
3.1.2.4. Layer 4: The transport layer.....	13
3.1.2.5. Layer 3: The network layer.....	14

3.1.2.6.	Layer 2: The data link layer.....	14
3.1.2.7.	Layer 1: The physical layer.....	15
3.2.	The TCP/IP Reference Model.....	15
3.2.1.	Layer 4: Application Layer.....	16
3.2.2.	Layer 3: The Transport Layer.....	16
3.2.3.	Layer 2: The Internet layer.....	17
3.2.4.	Layer 1: The Network Access layer.....	17
3.3.	Comparison between OSI and TCP / IP.....	18
3.3.1.	SIMILARITIES.....	18
3.3.2.	DIFFERENCES.....	18
4.	IP addressing	19
4.1.	Structure of IP addresses.....	19
4.2.	Classes Of IP Address.....	19
4.2.1.	Class A.....	19
4.2.2.	Class B.....	20
4.2.3.	Class C.....	20
4.2.4.	Class D.....	21
4.2.5.	Class E.....	21
5.	MAC Address	21
6.	Encapsulation	22
7.	IPv6 (Internet Protocol Version 6)	22
8.	Conclusion	23
 Chapter 02 : wireless ad hoc network		
1.	Introduction	24
2.	Wireless Networks	24

3. The Reference Model (IEEE 802)	25
3.1. Data link layer.....	26
3.1.1.Logical Link Control (LLC).....	26
3.1.2.Media Access Control (MAC).....	26
3.2. Physical layer.....	26
3.2.1.The Physical Layer Convergence Protocol (PLCP).....	26
3.2.2.Physical Medium Dependent (PMD).....	27
4. IEEE 802.11 Standards	27
5. Characteristics of The IEEE 802.11	28
6. Modes of wireless networks	29
6.1. Infrastructure mode.....	29
6.2. Ad hoc mode.....	30
6.3. The characteristics of Ad Hoc networks (MANET).....	31
6.4. The advantages and disadvantages of Ad Hoc networks.....	32
6.4.1.ADVANTAGES OF AD HOC NETWORKS.....	32
6.4.2:DISADVANTAGES OF AD-HOC NETWORK.....	33
6.5. ROUTING IN AD HOC NETWORKS.....	33
6.5.1.CLASSIFICATION OF ROUTING PROTOCOLS.....	33
6.5.1.1. PROACTIVE (table driven) ROUTING PROTOCOLS.....	34
6.5.1.2. REACTIVE (On Demand) ROUTING PROTOCOL.....	34
6.5.1.3. Hybride ROUTING PROTOCOL.....	35
6.5.2.ROUTING PROTOCOL.....	35
6.5.2.1. OLSR (Optimized Link State Routing Protocol).....	36
6.5.2.2. AODV (Ad hoc On demand Distance Vector).....	37
6.5.2.3. ZRP (Zone Routing Protocol).....	38

7. APPLICATIONS OF MANET.....	39
8. LIMITATION OF MANET.....	40
9. Conclusion.....	41
Chapter 3 : Security in wireless ad hoc network	
1. Introduction.....	42
2. Security.....	42
2.1. Definition of security.....	42
2.2. Security Objectives.....	42
2.3. Threats of ad hoc networks.....	43
2.3.1. Internal Attacks.....	44
2.3.2. External attacks.....	44
2.3.2.1. Passive attacks.....	44
2.3.2.2. Active Attacks.....	44
2.4. TYPES OF ACTIVE ATTACKS.....	46
2.4.1. Attacks at Network Layer.....	46
2.4.1.1. Blackhole Attack.....	47
2.4.1.2. Wormhole Attack.....	49
2.5. Security Solutions.....	50
2.5.1. Cryptography.....	50
2.5.2. Decentralized authentication of new nodes.....	50
2.5.3. Per-packet and per-hop authentication.....	51
2.5.4. Intrusion detection in manets.....	51
3. Computer security related risks.....	51
3.1. The security risk analysis.....	51
3.1.1. Sensitive functions and sensitive data.....	52

3.1.2. Wireless Networks Ad Hoc Security Requirements.....	53
3.1.3. Vulnerability.....	54
3.1.4. Threats.....	54
3.1.5. Result of The analysis.....	55
4. Ad hoc On Demand Distance Vector (AODV) Routing Protocol.....	55
4.1. Routing tables.....	56
4.2. Control messages.....	56
4.2.1. Routing request.....	56
4.2.2. Routing reply.....	57
4.2.3. Route error.....	58
4.2.4. HELLO messages.....	58
4.2.5. Route discovery.....	58
4.2.6. Reverse path setup.....	59
4.2.7. Forward path setup.....	59
5. Quality of service.....	59
6. Conclusion.....	61
Chapter 4 :Simulation	
1. Introduction.....	62
2. Simulation environment.....	62
3. The simulator NS2.....	62
3.1. Features of NS2.....	63
3.2. Advantages of NS2.....	63
3.3. Limitations of NS2.....	63
3.4. Installation de NS2 2.34 allinone.....	64

3.5. Simulation Steps.....	64
3.5.1.Preparation phase.....	64
3.5.2.Simulation Phase.....	65
3.5.3.Analysis Phase.....	65
4. Simulation.....	66
4.1. Implementation.....	66
4.2. Adding a new protocols in NS2.....	66
4.2.1.BLACKHOLEAODV/ IDSAODV.....	68
4.3. Simulation the protocols in ns2.....	70
4.3.1.The performance metrics.....	70
4.3.2.Simulation parameters.....	70
4.3.3.The simulation scenarios.....	72
4.3.4.Simulation Results.....	72
5. Conclusion.....	74
General introduction.....	75
Bibliography.....	76

General Introduction

The Security mechanisms that used in wired and conventional wireless networks and which are based on a centralized infrastructure are not appropriate to an ad hoc network completely decentralized. The solutions that have been developed trying to adapt the nature of ad hoc networks are costly, slow and consume a lot of resources (energy, computing power and storage) ,Which degrades the overall performance of the network. In this work, we focus on the security problems of routing protocols in ad hoc networks. For this, we have conducted a first study that focuses on the security mechanisms that have been proposed, and which are at present in order to ensure optimal routing and secure data exchange in ad hoc networks.

Following to this study, our interest is particularly focused on routing protocols whose role is to maintain permanently routing linkages. This task is difficult because of mobility and autonomy of the nodes of MANET networks, It uses therefore, to establish mechanisms and maintaining links inducing for some protocols, a decline in network performance. our choice was made on the AODV routing protocol who considered as one of the main most used in ad hoc networks routing protocols.

Indeed most of the proposed solutions are based on very complex cryptographic mechanisms, slow, and very costly in terms of resource consumption for authentication of communicating entities. These solutions are not very suitable for the ad hoc environment, and significantly degrade the performance of the basic routing protocol AODV. So our objective is to provide an effective security solution at low cost without significant degradation of network performance to obtain a good level of security and greater protection in the network, we have integrated our security scheme in the protocol IDSAODV. This last is a security extension of AODV protocol.

Planning for our work:

We will organize this memory into four chapters. In the first chapter we will make a general study on Protocols and Communication Architectures .Then we will take a look on wireless ad hoc network in the second chapter .Then we will present the security in wireless ad hoc network in The third chapter and finally in the fourth chapter for implementation and simulation our work.

General Conclusion

The security of routing in Ad hoc networks is a major problem, It's difficult to offer relatively robust mechanisms deal with different possible attacks, caused by external intruders and compromised nodes without affecting the overall performance of ad hoc network and routing protocols so too pronounced.

In this thesis, we were interested in analyzing the attack of Blackhole, we implemented two new protocols one for implementing the attack and the other for implementing an approach to prevent this attack related to sequence number, with this value the protocol detect suspicious behavior of Blackhole attacks. To evaluate the performance of the protocols, we have implemented them under the NS2 simulator. Next, we performed a series of simulations and we presented and interpreted the results.

This project gave us the opportunity to work under Linux environment, discover the simulation tool NS2 networks, discover and enrich our knowledge in Ad hoc wireless networks and network security in general.

At the end of this research, we can say that the security of routing protocols in ad hoc networks remains a real challenge. And Research will continue in this area to improve and optimize more and more existing security solutions to make ad hoc networks more reliable, more efficient and secure at low cost for the general public.

Future work

As future work, we intend to perform the solution for the black hole attack and apply this with different routing protocols like DSR and AOMDV and making a comparison between them .

Bibliography

Books

- [01] LES MCLELLAN, DEAN WHITTAKER, SANDY WORKMAN THE OSI REFERENCE MODEL
- [02] Padmini Misra Routing Protocols for adhoc mobile wireless networks
- [03] Valérie Gayraud & Bruno Tharon Securing Wireless Ad Hoc Networks, March 2003
- [04] Youngsik Lim The limit of ad hoc networks to commercial success (Position Paper) Electrical and Computer Engineering,

Articles

- [05] Aditya Bakshi, A.K.Sharma, Atul Mishra Significance of Mobile AD-HOC Networks (MANETS) ,(IJEIT) Volume 2, Issue 2, August 2012.
- [06] Ei Ei Khin, Thandar Phyu Comparative Analysis of Black Hole Attack Solutions in AODV Protocol ,(IJCCER) Volume 1 - Issue 2 July 2013.
- [07] Gagandeep, Aashima, Pawan Kumar Analysis of Different Security Attacks in MANETS on Protocol Stack A-Review , (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.
- [08] Mohammed Humayun Kabir, Syful Islam, Md. Javed Hossain, Sazzad Hossain Detail Comparison of Network Simulators , International Journal of Scientific & Engineering Research, Volume 5, Issue 10, October-2014.
- [09] Prashant Kumar Maurya, Gaurav Sharma , Vaishali Sahu, Ashish Roberts, Mahendra Srivastava Ad hoc network- An Overview , (IJMER), Pp-27-29, ISSN: 2249-6645 .
- [10] Sumeer Kumar, Sumit Kumar Various Solutions for Security in MANET A Review , International Journal of Enhanced Research in Management & Computer Applications, Vol. 3 Issue 10, , pp: (1-5), October-2014.

Memoirs

- [11] KADRI Benamar Mobile Ad hoc Networks Management Routing, Novembre 2012 and Security and MAHDJOUR HICHEM security in adhoc network ,juin 2013

Websites

- [12] www.techopedia.com, visited on 21/02/2015
- [13] www.wifinotes.com , visited on 21/02/2015
- [14] www.etutorials.org, visited on 22/02/2015
- [15] en.kioskea.net, visited on 10/04/2015
- [17] www.tutorialspoint.com, visited on 02/03/2015
- [18] www.omniseu.com, visited on 27/02/2015
- [19] technet.microsoft.com, visited on 02/03/2015

الملخص

تلعب الشبكات الاسلكية الخاصة في الوقت الحاضر دورا حيويا لتسهيل التواصل بين الجهات المختلفة لأغراض مختلفة, كما يعتبر الجانب الأمني من أكبر مصادر القلق في هذه الشبكات نظرا لنقاط الضعف الكثيرة في بروتوكولات التوجيه المعرضة لعدة هجمات قد تؤدي لاجداث خلل في الشبكة, من بين هذه الهجمات هجوم الثقب الأسود المنتمي لهجمات العقد الخبيثة و الذي قمت بتركيز دراستي عليه .

الكلمات الدلالية : الشبكات الاسلكية / أمن بروتوكولات التوجيه / هجوم الثقب الأسود.

Abstract

Now-a-days, wireless ad hoc networks (MANETs) are playing vital role for facilitating communication between different entities for different purposes. In case of wireless ad hoc networks security aspect has now becomes a very major concern and most of the current researches are focusing in the same direction .However, Due to security vulnerabilities of the routing protocols, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. One of these attacks is the Black Hole Attack which I have made my study on it.

Key words: MANET / routing protocols security / black hole.

Résumé

En ces jours, les réseaux sans fil ad hoc (MANET) jouent rôle essentiel pour faciliter la communication entre les différentes entités à des fins différentes. Mais les plus grandes menaces pour le réseau est l'aspect de la sécurité, cependant, en raison de failles de sécurité des protocoles de routage, réseaux sans fil ad hoc peuvent être sans défense contre les attaques par les nœuds malveillants. Une de ces attaques est l'attaque Black Hole que je l'ai fait mes études à ce sujet.

Mots clés : réseaux sans fil ad hoc / sécurité des protocoles de routage / Black Hole.