Département de mathématiques et Informatique

Travail personnel de l'Etudiant (TPE) ***Système et logiciel en environnement Distribué (SLED)***

19 Mars 2017

Security in mobile ad hoc networks: challenges and solutions

VANDI TIZE

10A665FS

NGOTCHIE CHRISTIAN JOEL

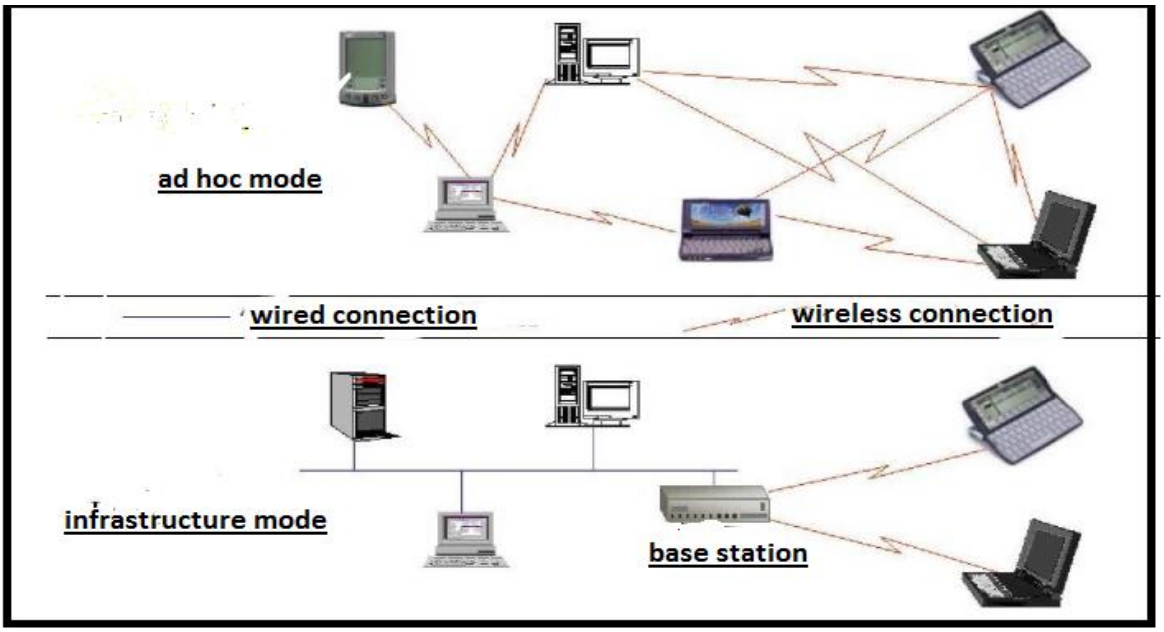
13A031FS

Supervisor : Dr-Ing. **FRANKLIN TCHAKOUNTE**

1-INTRODUCTION

1.1 CONTEXT

The Mobile Ad hoc NETwork (MANET) are wireless networks, with no existing infrastructure and distributed control. They are composed of various computing systems, more or less complex, called "nodes" with the possibility to communicate autonomously by radio waves. The mere fact of putting these nodes within radio range of each other will lead to the spontaneous appearance of a network (hence the name "spontaneous" sometimes given to the ad hoc networks), which makes it easier and faster to The installation of this type of network. The topology of these networks evolves as nodes move and rejoin or leave the network. Each node on the network serves as a terminal node and a routing point. The ad hoc mode of operation differs from the infrastructure mode in which the nodes of the network communicate with each other via an access point also called a "base" which can be connected to a fixed network.



The applications of such networks are numerous and tend to multiply with the miniaturization of processors and the diversity of terminals (sensors, mobile phone, laptop, PDA). These applications range from military operations, to sports event covers and emergency operations in the event of accidents or natural disasters. Simply put, a working meeting may request Creation of a computer network between its participants. Networks also represent a wide-ranging field of application. The organization of an evening of video games in network or each one brings its material, illustrates another application in this environment.

Many of challenges facing MANETs can be summarized as follows**:** the **node roaming in a hostile environment** (a battlefield for example) **the relative poor physical protection**

have non-negligeable probability of being compromised and we should not only consider malicious attack from outside a network ; use of wireless links renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion. In MANET security is compromise when the adversary successful to delete messages, to inject erroneous messages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation.

1.2 BACKGROUND

The expression 'Ad-hoc' is a Latin word means 'for this' or for this only that in wireless network computer indicate the collection of mobile nodes forming short live or temporary network without the aid of any centralized structure.

- **Origin of mobile ad hoc network**

In 1973 the Defense Advanced Research Projects Agency (DARPA) initiated research on the feasibility of using packet-switched radio communications to provide reliable computer communications. After a few year, this projects includes network protocols and protocols for automatic distributed network management.

- **First generation of mobile ad hoc network**

This generation introduce the utilization of radio frequency technology to transmit and receive data and the notion of firmware. The firmware in each packet radio gathers information about bidirectional link quality, nodal capacity and route characteristics and provides this knowledge to debugging and monitoring. The routing protocols used in packet radio network are designed to enable reliability, speed and correctness and thus include network management facilities, the result of this network management is the DARPA packet radio network can be installed and deployed quickly and easily.

- **Second generation of mobile ad hoc network**

During the years 1980-1993 mobile ad hoc network was be able to providing packet switched networking to the mobile battlefield element in infrastructure-less environments.The Global Mobile Information Systems (GloMo) project play an important role in the Second generation of mobile ad hoc network, The goal of the project is to make the mobile environment a firstclass citizen in the Defense Information ifrastructure by ^roviding user friendly connectivity and acess to services for wireless mobilr users.

- **Third generation of mobile ad hoc network**

1990, s-onwards, to mark by the Invention of notebook computers and viable communication devices based on radio waves concept of commercial ad hoc network has arrived and we see two main and important applications of mobile ad-hoc networks : Bluetooth and Ad-hoc sensors.

1.3 PROBLEM AND RESEARCH QUESTION

Constrains facing mobile ad hoc network concern the **data routing** through the network, that can be affected by: **The constant change of the network topology**, the entry into service or the **decommissioning of a node.** As other constraints we can have the ***communication channel access***, ***node mobility*** which affects the transmission of the signal, the ***routing*** and ***power consumption***. These constraints introduce many security problems in ad hoc networks such as passive listening, message interception or interception, network availability, packet integrity, and authentication and/or authorization user access.

These different problems offer many fields of research in terms of efficient bandwidth, the performance criteria in MANET (optimize throughput, reduce energy consumption), to optimize data routing and channel access, to deal with (manage) mobility.

2. RELATED WORKS

WORK	SECURE ROUTING	DATA CONFIDENTIALITY	DATA INTEGRETY	AVAILABILITY	USER AUTHENTIFICATION
[3]	✓			✓	
[4]					
[5]	✓				✓
[6]	✓				
[7]	✓				✓
[8]	✓	✓	✓	✓	✓
[9]		✓		✓	
[10]	✓	✓			
Routing protocol for the mobile ad hoc network	✓		✓		✓
Protocol de gestion de la confiance et de la réputation adapté aux réseaux ad hoc	✓				✓
Anomaly detection in NIDS		✓	✓		✓
Routing table update using oneway hach fonction					

	✓	✓			✓
ZRP, *DSR*, *TORA* and *AODV*	✓			✓	✓
Certification Authority		✓	✓		
Network intrusion detection systems NIDS		✓	✓		
Optimizetd link state routing (OLSR)	✓				✓
Ad hoc On Demande Distance Vector (AODV)	✓			✓	✓
WLANs	✓	✓	✓	✓	✓
single-hop and multi-hop topologies	✓			✓	
directional antennas and node transmission range	✓			✓	
proactive routing protocols and reactive on-demand routing protocols	✓			✓	✓
sleeping state	✓			✓	
Bloom filters		✓	✓	✓	
route messages	✓				
cluster-based intrusion detection technique for ad hoc networks		✓	✓	✓	✓

3. METHODOLOGY EMPLOYED

Security is an important issue for ad hoc networks, especially for those security-sensitive applications. This type of network is exposed to numerous attacks aimed at compromising both the security of the equipment and the data passing through it, these attacks can come from inside as well as from outside the network. Several methods are used to overcome the problem of insecurity in ad hoc networks, manly: ***physical node protection, intrusion detection, secure routing***.

3.1 Protecting the physical integrity of nodes

The physical attack of a valid element of an ad hoc wireless network, causing the compromise of the node, raises itself as a weak point of these networks. The physical integrity of a network node thus proves to be an important element in the safety of MANETs. This securing can be done using resistant materials for the construction of equipment, keeping the knots in places that are inaccessible (physical of course) to the general public.

3.2 Intrusion detection technique

MANETs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, unlike their wired counterparts, cannot be secured. The concept behind intrusion detection is a surprisingly simple one: Inspect all network activity (both inbound and outbound) and identify suspicious patterns that could be evidence of a network or system attack.

When an intrusion (any set of actions that attempt to compromise the *integrety, confidentially, or availability of resources*) take place, intrusion prevention technique, such as encryption and authentication (using password or biometrics), are usually at the first line of defense. An intrusion detection system inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. In wireless network the Intruder can stay anywhere on the range and intrude unseen;

In signature detection, the IDS analyze the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS looks for a specific a jack that has already been documented.

In anomaly detection, administrator defines the baseline, or normal, state of the network traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.

3.3 secure routing technique

The node mobility cause important problems in the data routing and may cause link breakage requiring route updates in the MANET. Secure routing protocols cope with malicious nodes that can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information by impersonating other nodes. It conserved as an extension that can be applied to several existing reactive routing protocols (SRP). SRP is based on the assumption of the existence of a security association between the sender and the receiver based on a shared secret key negotiation at the connection setup. SRP combats attacks that disrupt the route discovery process. A node initiating a route discovery is able to identify and discard false routing information. Similarly to SRP, Ariadne assumes that each pair of commuicating nodes has two secret keys (one of each direction of the communication). "*Ariadne is a secure ad hoc routing protocol based on DRS and the TESLA authentification protocol*."

The Authenticated Routing for Ad hoc Network (ARAN) protocol is an on-demand, secure, routing protocol that detects and protects against malicious actions carried out by

third parties in the ad hoc environment, ARAN is based certificates, and assumes that nodes obtain certificates from a trusted certificate server before join the ad hoc network. ARAN utilize a route discovery procedure similar to AODV (Ad hoc On Demand Distance Vector). To secure the communication, route discovery exploits an end-to-end authentication stage that guarantees that only the destination node can respond to a route discovery packet.

The Secure Efficient Ad hoc Distance (SEAD) is a proactive secure routing protocol based on DSDV. SEAD dels with attackers that modify a routing table update messages. The basic idea is to authenticate the sequence number and the metric field of a routing table update message using one way hash function hash chains and digital signature are used by the SAODV mechanism to secure AODV.

The secure ad hoc routing protocols take the proactive and enhance the existing ad hoc routing protocols, such as DRS and AODV with security extensions. In these protocols, each mobile node proactively signs its routing messages using the cryptographic authentication primitives described above. This way, collaborative nodes can efficiently authenticate the legitimate traffic and differentiate the unauthenticated packets from outsider attackers.

4. RESULTS FOUND AND PERSPECTIVES

4.1. **Solutions for Physical Nodes Integrity**

The integrity of the nodes of the network depends strongly on the physical capacities of this node to withstand attacks which would make it possible to modify the operation of the node in order to corrupt it. Having the ability to boot from a floppy disk, USB flash drive, or CD-ROM from a self-service PC into an open network greatly corrupts the integrity of that node. Indeed, the OS (Operating System) of the node can then be "exchanged by a corrupted OS. One way to work around this problem can be done by setting up functions to highlight a physical attack on the element; such a function can be compared with a seal ensuring the inviolability of a mail. It implements notions of traceability of the attack.

4.2 Solution to combat free listening and interception of packets

To be able to listen on the network, the malicious node will intervene on the routing protocol to ensure that the traffic that it wants to listen passes by him. In order to combat this problem, two solutions are envisaged: *The authentication system and the reputation management system.*

- **Authentification**

Authentication ensures that the user or device that is trying to connect is actually what they claim to be. This authentication will allow us to ensure the integrity of the

message as well as its authenticity. The conventional means for ensuring the integrity and authentication of the messages exchanged by the nodes of a network are the use of digital signatures or MACs (Message Authentication code). Digital signatures rely on public key cryptography. A node has a public key that serves its correspondents to encrypt messages intended for it and the node decrypts my messages that it receives with its private key. Another solution is to use MACs. These are one-way mathematical functions dependent on a secret key which, from the original message, produce a condensed form of this message. These mathematical functions are such that it is difficult to find a message from its condensed or to produce two messages having the same condensed

- **The reputation**

One can distinguish two behaviors that can impair the functioning of the network: egoism and malevolence. A node becomes egoistic in order to preserve its resources (energy, bandwidth). It merely for example to stop routing packets or only small packets. A malicious node will work to lower the reputation of others, which will lead to their exclusion from the network (mainly in routing). As a solution, there can be mentioned a method using the monitoring of the neighboring nodes and adapting the routing accordingly. This method is based on the use of two distinct components, a watchdog that will monitor the neighbors and modify their level of confidence according to their behavior and a path rather who will take care to route the traffic only to the nodes that appear to be trustworthy

4.3 Solutions for availability

There is no way to counter a denial of service on the radio channel provoked by a powerful attacker with the means to effectively of the radio spectrum. Nevertheless, techniques such as frequency hopping allows to guard against attackers with smaller capacities. Indeed These techniques allow data transmission over a wide range of frequency spectrum. To be effective an attacker must therefore be able to blur the range of frequencies used.

5. MOST IMPORTANT PUBLICATIONS FOR THIS WORK.

[1] Wenjia Li and Anupam Joshi ” ***Security Issues in Mobile Ad Hoc Networks - A Survey*** ” University of Maryland, Baltimore County

[2] HAO YANG, HAIYUN LUO, FAN YE, SONGWU LU, AND LIXIA ZHANG ” ***SECURITY IN MOBILE AD HOC NETWORKS:CHALLENGES AND SOLUTIONS*** ”,
T O P I C S I N W I R E L E S S S E C U R I T Y , February 2004

[3] Imrich Chlamtac a, Marco Conti b,*, Jennifer J.-N. Liu ***c,*** ” ***Mobile ad hoc networking: imperatives and challenges*** ”, ELSEVIER Ad Hoc Networks 1 (2003) 13–64

[4] Dhanant Subhadrabandhu, Saswati Sarkar, Farooq Anjum, **RIDA:** ***Robust Intrusion Detection in Ad Hoc Networks***, *May 2005*

[5] Humayun Bakht, ***History of mobile ad hoc networks***, Liverpool John Moores University

[6] Anand Patwardhan, Jim Parker and Anupam Joshi, Michaela Iorga and Tom Karygiannis, **Secure** ***Routing and Intrusion Detection in Ad Hoc Networks***,

[7] Atul Patel, Ruchi Kansara, Dr. Paresh Virparia, ***A Novel Architecture for Intrusion Detection in Mobile Ad hoc Network,*** *(IJACSA) International Journal of Advanced Computer Science and Applications, Special Issue on Wireless & Mobile Networks*

[8] Lidong Zhou, Zygmunt J. Haas, ***Securing Ad Hoc Networks*** Cornell University Ithaca, NY 14853

[9] Jerome LEBESGUE,Christophe BIDAN,Bernard JOUGA , ***Les réseaux Ad hoc et leur problématique de sécurité.*** *Supélec Renne –Equipe SSIR, avenu de la Boulais 35510 CESSON SEVIGNE.*

*[*10] Drs. Baruch Awerbuch & Amitabh Mishra, **Introduction to Ad hoc Networks,** Amitabh Mishra & Baruch Awerbuch 2008

References :

[1] Wenjia Li and Anupam Joshi ” ***Security Issues in Mobile Ad Hoc Networks - A Survey*** ” University of Maryland, Baltimore County

[2] HAO YANG, HAIYUN LUO, FAN YE, SONGWU LU, AND LIXIA ZHANG ” ***SECURITY IN MOBILE AD HOC NETWORKS:CHALLENGES AND SOLUTIONS*** ”,
T O P I C S I N W I R E L E S S S E C U R I T Y , February 2004

[3] Imrich Chlamtac a, Marco Conti b,*, Jennifer J.-N. Liu ***c,*** ” ***Mobile ad hoc networking: imperatives and challenges*** ”, ELSEVIER Ad Hoc Networks 1 (2003) 13–64

[4] Dhanant Subhadrabandhu, Saswati Sarkar, Farooq Anjum, **RIDA:** ***Robust Intrusion Detection in Ad Hoc Networks***, *May 2005*

[5] Humayun Bakht, ***History of mobile ad hoc networks***, Liverpool John Moores University

[6] Anand Patwardhan, Jim Parker and Anupam Joshi, Michaela Iorga and Tom Karygiannis, **Secure *Routing and Intrusion Detection in Ad Hoc Networks*,**

[7] Atul Patel, Ruchi Kansara, Dr. Paresh Virparia, ***A Novel Architecture for Intrusion Detection in Mobile Ad hoc Network,*** *(IJACSA) International Journal of Advanced Computer Science and Applications, Special Issue on Wireless & Mobile Networks*

[8] Lidong Zhou, Zygmunt J. Haas, ***Securing Ad Hoc Networks*** Cornell University Ithaca, NY 14853

[9] Jerome LEBESGUE,Christophe BIDAN,Bernard JOUGA , ***Les réseaux Ad hoc et leur problématique de sécurité.*** *Supélec Renne –Equipe SSIR, avenu de la Boulais 35510 CESSON SEVIGNE.*

*[*10] Drs. Baruch Awerbuch & Amitabh Mishra, **Introduction to Ad hoc Networks,** Amitabh Mishra & Baruch Awerbuch 2008

[10] Humayun Bakht, ***History of mobile ad hoc networks,*** Liverpool John Moores University

[11] **Vincent GLAUME,** *Détection d'Intrusion Réseau et Système,* ***28/11/08***

[12] Jérôme LEBEGUE, Christophe BIDAN et Bernard JOUGA, ***Les réseaux ad hoc:***

problèmes de sécurité et solutions potentielles, Supélec Rennes - Equipe SSIR, 13 octobre 2005

[13] Marine Minier, ***Sécurité et réseau ad hoc, marine.minier@insa-lyon.fr.***

[14] Valérie Gayraud, Loutfi Nuaymi, Francis Dupont, Sylvain Gombolt and Bruno tharon, ‘’***La sécurité dans les Réseaux Sans Fil Ad Hoc’’,*** Thomson R&I, Security Lab, Avenue de belle-Fontaine