Security in mobile ad hoc networks (MANETs) and WSNs (Wireless Sensor Networks)

Sami El Jay[1], **Abderrahim Hasbi**[2]
RSI, LRIE, Ecole Mohammedia d'Ingénieurs (EMI), Université Mohammed V

Abstract
we are moving towards an era where the majority of the objects accompanying our daily lives have become connected. Because of their small size, the facility of deployment and their reasonable cost, small wireless components have become increasingly popular among industrialists, users said nomads and in several areas that we will cite later. A network of such objects, commonly called MANETs such Mobile Ad hoc NETworks still a new paradigm among users of wireless network. Despite the advantages that these types of networks bring, their architecture remains powerless to several types of attacks. In this article we intend to do a literature review on MANETs, exactly on the safety of the MANET. For this, we will start with an overview of MANETs and their application areas. We will later focus on security challenges, become a major objective to deploy a such network since it carries information that can sometimes be confidential or personal (eg in the military or health). Then we will see the Resource Exhaustion attack, which can disrupt a network and isolate a network. We will talk later about solutions that had been done to prevent this attack and propose an approach to prevent againt Resource Exhaustion attacks. And to close this article, we will make a conclusion that summarizes the current state of security in ad hoc networks, proposing some ideas that seem relevant to enhance the security policy in MANET networks.

Key-words
MANETs, secure routing, resource exhaustion, AODV, ns2 …

1. Introduction

Wireless ad hoc Network is a collection of mobile nodes which move in an unpredictable manner in a given territory [1]. Based on wireless technology as a transmission medium, such devices are alone responsible for the creation, management and maintenance of the network. Unlike other types of wireless networks, such as cellular or 802.11 networks, which requires a fixed infrastructure that manages and maintains the network, a mobile ad hoc network can be born and exist without the intervention of any human intervention or a pre-existing device.
The flexible characteristics of ad hoc networks have given them a big boost within the scientific and industrial community, compared to other wireless networks and mobile cited above [2].

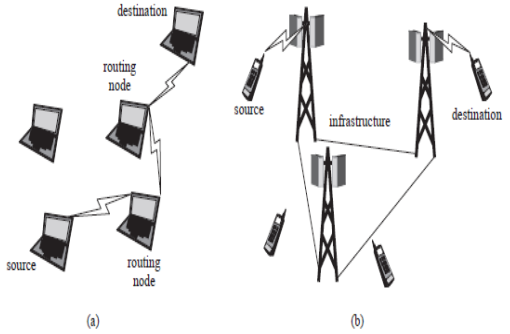

Figure 1: (a) Ad hoc Network, (b) Cellular Network

Because of their wireless communication and the lack of a management infrastructure, security challenges become more severe to prevent, since nodes deployed in a non-monitor environment, they can be easily compromised. Therefore, the attacker can read, delete or change data that can sometimes be confidential. However, the biggest challenge of ad hoc networks is that of security. Securing a wireless network, with limited resources and without energy management infrastructure is a challenging task. In this article, we will discuss Denial of service (DoS) attacks that aim to degrade the network resources and to disrupt services network [3]. Several researches have been done in this topic [4] [5] in order to popularize this type of network. DoS attacks could be considered as major threats against an ad hoc network and specifically against a WSN. DoS attacks can occur in any layer of the OSI model and her events aim to disrupt or totally destroy a network [6].
For this, any event that attempts to reduce the capacity of a network or prevent an action to take place is considered as a DoS attack, although node responsible for this action is a legitimate node. Several types of DoS attacks exist in the literature [7], ranging from attacks that affect the physical layer of the OSI model to the transport layer. In the following, we will focus on the attack "Resource Exhaustion" which manifests itself at the data link layer.

Manuscript received September 5, 2016
Manuscript revised September 20, 2016

2.Manets Applications and challenges

Multiple domains have adopted ad hoc networks seen the benefits that they can offer and especially when deploying a wired network infrastructure is costly or impractical. The first implementations of MANET networks have emerged in the military within the US Department of Defense since the beginning of 1970s. This allowed the army to communicate in the battlefield and maintain the flow of information between soldiers, military vehicles and all devices connected to the network.

In the commercial sector, mobile ad hoc networks can be used as a tool to help and monitoring data by sending panic alarms result of a disaster, an earthquake, fire or flood. In the area of medicine where doctors can monitor the health of the patient to which a connecting chip has been graft and that makes transmitting the data collected in real time indicating the patients' health. Other applications can implement a MANET network such as the field of automotive, where each vehicle is equipped with several sensors that communicate with the sensors that are placed along the road, and with the sensors of other vehicles in order to route and share useful information for traffic management. Called VANET network, this particular case the ad hoc network aims to improve the state of the road traffic and reduce the rate of accidents. In the civilian sector, end users can also implement an ad hoc network in a quick and instant way in order to share real-time information, such as the case of a conference or meeting.

Nevertheless, despite the multitude of benefits that can provide a mobile ad hoc network in several application areas, their architecture suffers from a number of challenges that must be addressed [3]. The first challenge, which has become the major concern of the ad hoc networks, especially sensor networks, is the data security. With a wireless transmission medium, data can easily be captured, analyzed, modified, and well see deleted.

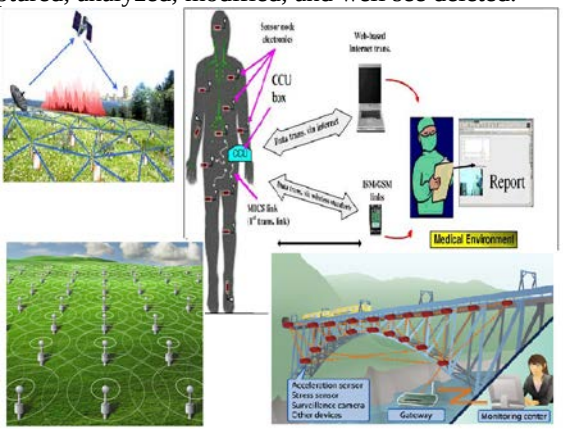

Figure 2: MANETs applications

In addition to the most common vulnerabilities in wireless networks, such as passive listening [9], data tampering, identity theft, denial of service attacks and other MANETs are vulnerable to many other attacks because of their mobile architecture, low energy and their relatively small physical protection [8].

The entity node in this network plays a pivotal role, since each node is responsible for routing data to each other in the network, following the principle Store and Forward [9]. So, destruction or manipulation of a node by an anonymous third party can cause real damage. In addition, the use of batteries as a power source provides an opportunity for evil spirits to launch DoS attacks, forcing nodes to make expensive additional calculations and transmissions to exhaust their batteries.

The second and main challenge for mobile ad hoc networks is that of energy. Nodes are deployed with limited energy sources as often irreplaceable integrated batteries whether the operating range is difficult to achieve. The management and optimization of the battery is an essential task to keep estimated life of the network.

The third major challenge is the nodes mobility in a MANET network. This generates a topology change, i.e. a change of the routing data. So routing algorithms must ensure that the routing tables are updated in a permanent way in order to avoid frequent breakdowns of communication links and then, packet loss.

As Sun Tzu said in his book entitled Art of war [4], win or lose a war does not happen by chance. It is a matter of good principles and methods that lead to victory. According to R. Di Pietro, S. Guarino in their article [7] in a higher level, the attacks against MANETs can be classified according to the state of the attacker, behavior and goal of the attack. So for perfect security of data circulating within an ad hoc network, several network protocols must be adequately capable of detecting these three criteria mentioned earlier in a given attack that attempt to disrupt network operation.

Several types of attacks are known in the literature of ad hoc networks. Generally, these attacks are classified two major categories, active and passive attacks. In the following, we will see in detail the different types of attacks that exist for ad hoc networks and we will focus specially on the attack "resource exhaustion".

Passive attacks, act by listening and analyzing information captured -or touted since it is a not honest action- without alter or modify the contents of messages. Unlike, the so-called active attacks, that affect not only the confidentiality of data, but also their integrity. This type of attack can lead to a disruption of communications in the network following the modification of routing messages and useful messages, or a deletion or injection messages which requires intensive use of destination node resources until exhaustion.

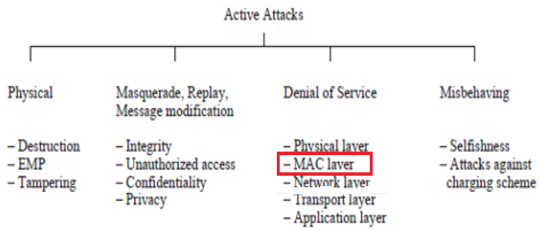

Figure 3: Active attacks

Resource Exhaustion or resource depletion [6] is an active attack known for several years, which falls into the category of DoS attacks. The attack Resource Exhaustion affects data link layer and occurs when a resource node, responsible for performing a particular action is entirely consumed [7]. This attack of denial of service is easy to implement, but difficult to prevent. It is sufficient for the attacker to inject a number of unneeded packets, which encourage nodes to make additional calculations and accelerates the process of resource consumption. This additional packet paralyzes a part of the network, when the bandwidths that the legitimate nodes should use to transfer their data are completely unavailable. To launch this attack, the attacker should have diverse knowledge about of MAC protocols functioning. For example, an attacker can send a RTS message to the target node in order to prompt a CTS response from him and implicitly, exhaust node resources.

3. Related Works

The denial of service attacks, are attacks that have been known in the computer networks a long time ago [9]. Or classic secure routing protocols against this type of attack is not applicable for MANETs seen their different characteristics. Several studies have been performed in this direction to improve existing or designing new protocols to protect the network against malicious attempts of "Resource Exhaustion" attacks [10] [11]. Nevertheless, security solutions for the MANET routing protocols are insufficient and still unable to resist this type of attack. In this part of the paper, we will make an overview of the work that has already been done and that demonstrate a considerable effort, to implement a strong and effective security approach. We'll start with the work of Qijun Gu, Liu Peng, Chao-Hsien Chu and Sencun Zh, who suggested a on demand hop-by-hop protocol named Source Authentication Forwarding or FAS [12] allows the source authentication for the data transfer. This research answer a very interesting problem that prevents the implementation of the authentication mechanism in MANETs, and this is due to the high mobility of nodes and the sudden change in the topology. FAS protocol allows each node to check each received packet before transmitting it to the next node. In other words, the source authentication is performed on each hop in order to filter the injected packets. It is based on the DSR protocol because it requires the IDs of the nodes in the transmission path. To avoid exhaustion attack, this protocol uses authentication jump-by-jump in which three steps are required: Their algorithm allows authentication of the source during the data transfer. This research addresses a very interesting problem in MANETs, which prevents the application of the authentication mechanism in MANETs because of the high mobility of nodes and the abrupt change of the topology. FAS protocol allows each node to check each received packet, before transmitting it to the next node. In other words, the source authentication is performed on each hop in order to filter the injected packets. It is based on the DSR protocol. To avoid exhaustion attack, this protocol uses authentication jump-by-jump in which three steps are required:

3.1 Pairwise Keys Establishment :

The source node sets up a pairwise key with every en route node along the path, based on IDs of routing nodes obtained from DSR route reply packets.

3.2 Authentication :

When a source node S wants to send data packets to destination D through a route of n-1 routing nodes, S attaches an authentication header $A(i)$ to each data packet $PKT(i)$.

$$A(i) = SID(i)||PC(i)||\delta_{R1}(i)||\delta_{R2}(i)||\dots||\delta_{Rn}(i)$$

$SID(i)$ is the source ID, $PC(i)$ is the count of the packet and $\delta_{Rn}(i)$ is the authentication token for Rn.

3.3 Forwarding:

In a route, each node set a forwarding entry, which extends a routing entry to store information for verifying received packets. Another research by MASAO TANABR and AIDA MASAKI [13], n their report, they present three methods to prevent the attack of Resource Exhaustion. The first method uses the time slot, in this method; each legitimate node must send its packets in its pre-assigned time slot. The second method uses tokens; in this approach each terminal can transmit its packet only if he receives a token from the network. The third method use cryptography schemes, based on symmetric encryption, each node that wants to send data may encrypt packet with the secret key. In their paper, MASAO TANABR and AIDA propose a highly secure method of communication in MANETs that prevents the Resource Exhaustion attacks.

4. Approach

Data partitioning provides a solution to prevent intruder's node to retrieve the information circulating in ad hoc network and prevent against Resource Exhaustion. The principle of the approach is to divide the information into several fragments; each fragment is transmitted via a different path. When a node of ad hoc network wants to send data, this node will fragment the information into multiple packets (figure 4) of a fixed size by assigning each packet a sequence number to be encrypted at the source node and decrypted at the destination node. These packets are then sent over different transmission links and will be received by the destination node, which will then collect them to rebuilt information.

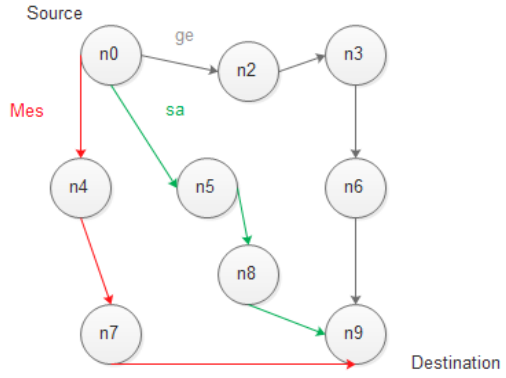

Figure 4: Message Fragmentation in Ad hoc Networks

With this approach the fragmentation of messages, we can reduce the impact of resource exhaustion attack, in addition to the message corruption and the dropping of the packets due to the presence of malicious nodes on some of the paths or unavailability of one of the paths due to breakage will have no affect on the data transmission, provided most of the pieces are received by the receiver. Each packet is analyzed by the destination node to extract the encrypted ID, and it can eliminate all the malicious packets that not have an encrypted part ID, and want to introduce network for injecting false data, which disrupts routing tables.

This approach would be an entry point for our future research. Fragmenting the data before sending enhances network security to prevent against resource exhaustion and towards other several attacks, such as data replication, the black hole attack, gray hole attack-Forwarding Selective, worm whole attack and Sybil attack [14].

5. Simulation

In this work, we worked on the ns2 simulator [15]. In this section, we demonstrate our choice for the AODV routing protocol for testbed.

Ns2 is an open source object-oriented network simulator, designed in 1989. It is written based on the C + + language with an interpreter otcl. Ns2 is then composed of two complementary languages. C++ defines the internal mechanism of the simulation objects, which implements the otcl simulation assembly and configuration objects. All C++ code must be compiled and linked to create an executable file. The ownership of the C++ language is that quick to run, but slower to change. Otcl is slow to run and to reflect changes. So NS2 is built on the basis of the advantages of the two languages.

The following figure shows the remaining energy of a specific node while it is a resource exhaustion attack. In our research, we are using the AODV protocol for built and maintain routes between nodes. Our choice of AODV is based on several reasons. AODV is one of the most efficient routing protocols in terms of establishing the shortest path and lowest power consumption. It is mainly used for ad-hoc networks but also in wireless sensor networks. It uses the concepts of path discovery and maintenance. However, AODV builds routes between nodes on demand i.e. only as needed. For demonstrating our choice, the next figure shows the remaining energy of a specific node under a Resource Exhaustion attack. We realize a comparison with multiple routing protocols that are AODV, AOMDV, DSDV, DSR, PUMA and TORA.

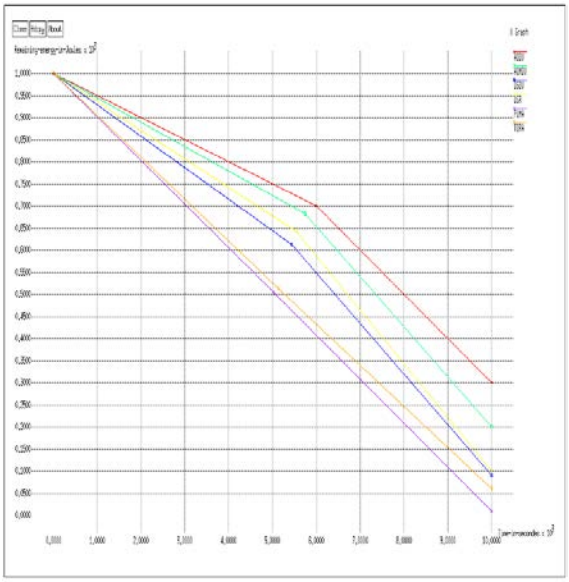

Figure 5: Remaining energy of a specific node while it is under a resource exhaustion attack

As we can see, the AODV protocol (the red line) is more energy efficient. We then thought to adopt this protocol in our future research in order to secure against resource exhaustion attack.

6. Conclusion and Future Works

Securing an ad hoc network is not a simple task. First of all, algorithm that secures the network must ensure the authentication procedure. In other words, ensure the process that aim to confirm that a committing is the node that he claims to be. In this way, we will be certain that all the participants in a discussion are legitimate entities. The identity of each committing is confirmed based on four traditional factors of authentication, which can be used to confirm the identity of a committing:

- Use Information that only the committing knows.
- Use Information that only the committing features.
- Use Information that characterizes the committing in a given context.
- Use Information that only the committing may occur.

Other authentication factors can sometimes be used as time constraints or location capabilities. But it cannot guarantee non-repudiation of message.

References

[1] R. Hekmat, Ad hoc Networks : Fundamental Properties and Network Topologies, The Netherlands.: Springer, 2006.

[2] J.-Z. Sun, «Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing,» Finland.

[3] W. D. a. C. Poellabauer, FUNDAMENTALS OF WIRELESS SENSOR NETWORKS THEORY AND PRACTICE, WILEY, 2010.

[4] C. B. a. M. L.-M. a. K. BEKARA, «H2BSAP:A Hop-by-Hop Broadcast Source Authentication Protocol for WSN to mitigate DoS Attacks,» IEEE, 2008.

[5] K. G. a. S.-H. Yang, «A Scheme for Preventing Denial of Service Attacks on Wireless Sensor Networks,» IEEE, 2009.

[6] A. K. M. A. G. N. G. Sunil Ghildiyal, «ANALYSIS OF DENIAL OF SERVICE (DOS) ATTACKS IN WIRELESS SENSOR NETWORKS,» IJRET: International Journal of Research in Engineering and Technology, vol. 03, Jun 2014.

[7] S. G. N. V. J. D.-F. R. Di Pietro, «Security in wireless ad-hoc networks – A survey,» Elseiver, 2014.

[8] Z. J. H. Lidong Zhou, «Securing Ad Hoc Network,» Cornell University.

[9] D. B. J. A. P. Yih-Chun Hu, «SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks,» Elsevier, vol. 1, pp. 175-192, July 2003.

[10] D. Martins, «Sécurité dans les réseaux de capteurs sans fil Stéganographie et réseaux de confiance,» UNIVERSITÉ DE FRANCHE-COMTÉ, 2010.

[11] S. Tzu, The Art of War, The Puppet Press, 1910.

[12] B. G. a. M. Minea, «Formal Modelling and Automatic Detection of Resource Exhaustion Attacks,» ACM, n° %1978-1-4503-0564-8/11/03, 2011.

[13] A. MISHRA, Security and Quality of Service in Ad Hoc Wireless Networks, Cambridge University Press, 2008.

[14] S. X. S. S. S. J. Sencun Zhu, «LHAP: A Lightweight Network Access Control Protocol for Ad-Hoc Networks,» Elsevier, vol. 4, pp. 567-585, 2006.

[15] P. L. C.-H. C. S. Z. Qijun Gu, «Defense Against Packet Injection in Ad Hoc Networks,» Inderscience Publisher, Texas State, 2007.

[16] M. A. MASAO TANABE, «Secure Communication Method Using Invitation Process in Mobile Ad hoc,» Tokyo, JAPAN, December 2012.

[17] K. V. Kevin Fall, «The ns Manual (formerly ns Notes and Documentation),» January 6, 2009.

[18] Les Réseaux Mobiles Ad Hoc & Les Protocoles de Routage.

[19] M. M. Bogdan Groza, «Customizing protocol specifications for detecting resource exhaustion and guessing attacks,» University of Timisoara.

[20] M. Guizani, Wireless Communications Systems and Networks, Academic Publishers New York, Boston, Dordrecht, London, Moscow, 2004.

[21] S.-J. L. W. S. a. M. G. Sang Ho Bae, «The Design, Implementation, and Performance Evaluation of the On-demand Multicast routing protocol in Multihop wireless networks,» IEEE, California, 2000.

[22] E. C. a. C. RONG, Security in Wireless Ad Hoc and Sensor Networks, Norway: Wiley, 2009.

[23] S. B. A. K. V. Gaurav Sharmaa, «Security Frameworks for Wireless Sensor Networks-Review,» chez ELSEVIER, India, 2012.

[24] P. N. Donggang Liu, Security for Wireless Sensor Networks, Springer, 2007.

[25] D. W. Chris Karlof, «Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,» Elsevier, Vols. %1 sur %2Volume 1, Issues 2–3, p. 293–315, 2003.

[26] M. T. a. M. Aida, «Preventing Resource Exhaustion Attacks in Ad Hoc Networks,» IEEE, 2007.

[27] D. V. C. D. Nikos Komninosa, «Layered security design for mobile ad hoc networks,» Elsevier, pp. 121-130, 2006.

[28] L. n. F. D. S. G. a. B. T. Valérie Gayraud, «La Sécurité dans les Réseaux Sans Fil Ad Hoc,» ENST Bretagne.

[29] W. D. a. C. Poelleabauer, Fundamentals of Wireless Sensor Networks Theory and practice, Wiley Series on Wireless Communications and Mobile Computing, 2010.

[30] A. D. W. a. J. A. Stankovic, «Denial of Service in Sensor Networks,» IEEE, n° %10018-9162, pp. 48-65, 2002.

[31] A. K. M. A. G. N. G. Sunil Ghildiyal, «ANALYSIS OF DENIAL OF SERVICE (DOS) ATTACKS IN WIRELESS SENSOR NETWORKS,» IJRET: International Journal of Research in Engineering and Technology, Jun 2014.

[32] M. D. S. Dr. G. Padmavathi, «A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,» (IJCSIS) International Journal of Computer Science and Information Security, pp. Vol. 4, No. 1 & 2, 2009.