Journal of Computer Sciences

Review

Generation Test-Cases of Attacks in Mobile Ad Hoc Network

[1]Sara Chadli, [2]Mohammed Saber and [1]Abdelhak Ziyyat

[1]Laboratory of Electronics and Systems, Faculty of Sciences, Mohammed First University, Oujda, Morocco
[2]Laboratory Electronics, Computer and Image Systems,
National School of Applied Sciences, Mohammed First University, Oujda, Morocco

Article history
Received: 04-07-2016
Revised: 25-11-2016
Accepted: 10-12-2016

Corresponding Author:
Mohammed Saber
Laboratory LSE2I, National School of Applied Sciences, Mohammed First University, Oujda, Morocco
Email: mosaber@gmail.com

Abstract: The number and increasing complexity of attacks against MANETs have grown significantly in recent years. While many security proposals have been developed. However, these proposals suffer from the problems of tests and evaluations. Among these solutions, the Intrusion Detection Systems (IDS) that can act as defense mechanisms. However, this last poses serious problems for its evaluators that need classify the attacks to select case test. In this paper, we make a thorough analysis of existing attack classifications in order to determine whether they could be helpful in selecting attack test cases. Based on our analysis, we construct a new scheme to classify attacks relying on those attributes that appear to be the best classification criteria. We also apply the Classification Tree Method (CTM) to select test-case to attack. Finally, we use the Classification Tree Editor (CTE) tool to generate and select test-case.

Keywords: MANETs, Classification, Attacks, Test-Case, Intrusion Detection System (IDS)

Introduction

The remarkable advances in technology have encouraged the development of mobile networks prodigiously. Ad hoc mobile networks are one of the main categories of mobile networks. Ad hoc mobile network is a distributed system consisting of several autonomous entities able to communicate with each other without the existence of a centralized infrastructure. These nodes communicate via radio frequencies and can self-organize and cooperate to provide services.

The widening application domain of mobile ad hoc networks requires more security to ensure the integrity and confidentiality of data traveling on the network. Indeed, mobile ad hoc networks are confronted with many problems related to their characteristics (absence of infrastructure, dynamic topology….), which make developed security solutions for wired and wireless networks with infrastructure inapplicable in the context of mobile ad hoc networks. In addition, the number and complexity of attacks against MANETs have experienced a significant increase in recent years. This poses serious problems for evaluation and testing of security solutions for MANETs and among these solutions systems intrusion detection.

However, the same argument that enabled a massive deployment of IDS, poses serious problems for evaluators of such systems. Indeed, how effectively test and be sure (prove) that the IDS behaves correctly (e.g., Alarm generation when an intrusion attempt, no false alarms, etc.) for all existing attacks? A solution that may seem trivial is to build relevant and representative classifications of all attacks.

Several researches address the classification of attacks in wired networks as (Hansman and Hunt, 2005; Paulauskas and Garsva, 2006; Saber *et al*., 2010). But in MANETs, there is no more work against attacks classification. Recent works in (Padmavathi and Shanmugapriya, 2009) have classified attacks mainly into two categories: Active or passive attacks and attacks in the different network layers (Mamatha and Sharma, 2010). Under each category, a list of attacks is presented. These studies do not allow a better evaluation and testing of security solutions.

The solution may seem trivial is to build classifications and representative of the attacks, in order to present a relevant approach for selecting test cases. The idea is based on the concept of equivalence class well known in the field of software testing. For this, we use a method based on the classification tree (CTM for Classification Tree Method). Finally, we use the tool Classification Tree Editor (CTE) to generate and select test cases.

This article is composed as follows: In the second section we will present the existing attacks classifications for MANETs. We detail our classification in the third section. In the fourth section, we present the results. We end with a conclusion and future work.

Related Works

Attacks against mobile ad hoc networks are classified into several categories according to several authors. This classification can be made according to various criteria such as: The effect of the attack or location of the attack in the different layers of the network.

Attacks Classification According to the Effect of the Attack

Depending on the attack effect, several authors (Awerbuch *et al*., 2002; Pietro *et al*., 2014; Sen *et al*., 2010; Singh *et al*., 2014) classify attacks in two different types: Passive or active (Table 1).

Active Attacks

An active attack is to alter or delete the data exchanged in the network causing a disruption in the normal operation of the network. Active attacks are interpreted by several actions such as: Identity theft, modification, deletion or replication of messages circulating in the network.

Passive Attacks

In passive attacks, there is no change on the information transferred in the network. However, the attacker can listen, recover or analyze traffic flowing through the network thus violating the confidentiality of information and the anonymity of the sender. The detection of this type of attack is difficult as the operation of the network itself is not unbalanced.

Attacks Classification Depending on its Location in the Different Network Layers

Several authors (Mpitziopoulos and Gavalas, 2009; Mamatha and Sharma, 2010; Amit *et al*., 2013; Murugan and Shanmugam, 2010) see that firstly it is necessary to identify the types of attacks according to the abstraction layer (at OSI sense) to protect themselves, because they see that MANET characteristics make them susceptible to many new attacks. These attacks can occur in different layers of the stack of network protocols (Table 2).

Physical Layer

A malicious entity without even having to take part in the ad hoc network can simply generate strong radio emission aimed to parasitize transmissions and making correct operation impossible.

Link Layer

Assuming the link layer is egalitarian; a node may well saturate the medium by transmitting control or data frames and thus prevent other nodes to communicate. This is called Denial of Service (DoS denial of service or English). Specific attacks on IEEE 802.11 MAC layer, which exploit some aspects of the protocol can also cause a denial of service.

Network Layer

It is at this level that operates routing protocols (Gopalakrishnan and Ganeshkumar, 2014; Mahdi *et al*., 2013) and data packets are broadcast. A malicious node can thus divert the normal operation of the protocol by issuing false information in his messages. It can also attack the data packets by destroying, altering or retransmitting them more than necessary.

Application Layer

Attacks at this level are common to all types of networks and their operating mode is specific to the particular intended application.

Table 1. Attacks classification according to the effect of the attack

Class	Attacks
Active	Jamming; Tampering; Node replication; Collision; Exhaustion; Unfairness; Sleep deprivation; Hello flooding; Black hole; Sink hole; Byzantine; Wormhole; Rushing; Selective forwarding; Routing table Poisoning; Sybil; Resource consumption; Traffic analysis; Packet injection; Packet duplication; Packet alteration; Routing information; Flooding; Desynchronization; Session Hijacking; Malicious code; Repudiation
Passive	Eavesdropping

Table 2. Attacks classification depending on its location in the different network layers

Layer	Attacks
Physical	Jamming; Tampering; Eavesdropping; Node replication
Link MAC	Collision; Exhaustion; Unfairness; Sleep deprivation
Network	Hello flooding; Black hole; Sink hole; Byzantine; Wormhole; Rushing; Selective forwarding; Routing table Poisoning; Sybil; Resource consumption; Traffic analysis; Packet injection; Packet duplication; Packet alteration; Routing information
Transport	Flooding; Desynchronization; Session Hijacking
Application	Malicious code; Repudiation

Table 3. Mapping of attacks in MANETs

			Target			Attacker		Attack	
Layer	Attack	Objective	Network availability and service integrity	Privacy and secrecy	Data integrity	Internal	External	Active	Passive
Physical	Jamming	Entirely disrupting a legitimate signal	×				×	×	
	Tampering	Steal confidential data and cryptographic material	×				×	×	
	Eavesdropping	Information confidentiality violation/Probe or scan		×			×		×
	Node replication	Information integrity violation			×		×	×	
Link MAC	Collision	Depleting the energetic resources of the nodes	×				×	×	
	Exhaustion	Depleting the energetic resources of the nodes	×				×	×	
	Unfairness	Degrading the timeliness of the service	×			×		×	
	Sleep deprivation	Depleting the energetic resources of the nodes	×				×	×	
Network	Hello flooding	Causing both data loss and energy wasting	×				×	×	
	Black hole	By inducing the nodes to route all the traffic through a set of compromised nodes, that can then drop (or access) all the routed packets.	×				×	×	
	Sink hole	Focuses on the routing pattern of a protocol The malicious node attracts the packets from the other normal nodes and drops the packets.	×				×	×	
	Byzantine	Routing protocols	×			×		×	
	Wormhole	Routing protocols	×				×	×	
	Rushing	Routing protocols	×				×	×	
	Selective forwarding	Degrades the network performance in terms of packet loss rate, collision and overhead	×				×	×	
	Routing table Poisoning	Routing protocols	×				×	×	
	Sybil	Routing protocols	×				×	×	
	Resource consumption	Depleting the energetic resources of the nodes	×				×	×	
	Traffic analysis	Information confidentiality violation		×		×		×	
	Packet injection	Information integrity violation and Data Overwrite			×	×	×	×	
	Packet duplication	Information integrity violation			×	×	×	×	
	Packet alteration	Information integrity violation and Data Overwrite			×	×	×	×	
	Routing information	Spoof, alter, or replay routing information	×			×		×	
Transport	Flooding	Exhaust the memory resources of a node	×			×		×	
	Desynchronization	Deplete the batteries of the nodes	×				×	×	
	Session Hijacking	Information integrity violation/Masquerading as another session			×		×	×	
Application	Malicious code	Attack both mobile operating systems and user applications.	×				×	×	
	Repudiation	refers to a denial of participation in all or part of the communication	×				×	×	

Analysis of Older Classification

We presented in this section, the existing attacks classifications in MANETs. Based on the study of these classifications, we deduced that the majority of attacks classifications for MANET have been designed to a specific goal; For example, understanding the vulnerabilities to reinforce the corrective and defensive measures, understanding the attack processes as well as the attacker's behavior.

In Table 3 we give summarizes the attributes of different attacks.

Presentation of the Proposed Classification

Objectives of the Proposed Classification

The objective of our classification is to provide a useful and coherent way which allows to know in advance the new attacks and to provide a structured way to take into account all part of attacks. Also the suggested classification should be open for expansion.

The resulting classes as well as the classification process must respect, as much as possible, the satisfaction characteristics studied in (Hansman and Hunt, 2005) which are:

- Fullness: A categorization outline must consider all possible attacks (known and unknown)
- Scalability: When some new attacks appear the categorization outline should allow classifying them their classification
- Criteria clarity: The classification outline and rules must be well-established in a way that an attack can be classified by taking just one class from each dimension
- Repetitiveness: The reimplementation of the classification process must always produce the same results; in other words, if we repeat the followed stages for a certain attack classification, we must always put it in the same category
- Conformity: With the standards and resulting terminologies; mainly, with vulnerability data bases and dictionaries which are nowadays widely used
- Mutual Exclusion: Be sure that an attack is not part of two different categories. Therefore, a dimension will that mutually exclusive classes

Description of Proposed Classification

The proposed classification is based on five dimensions, as shown in Fig. 1. These dimensions are

selected to cover the sources, targets and manifestations of the attacks, these dimensions are:

- Source: Indicating where the attack was launched. It has two classes: Local and remote
- Privilege: We distingue two classes of privileges under the attacker, the class "Authorized" means that the attacker was able to gain access to control node. The class "Unauthorized" covers attacks that do not require any access privilege system, such as recognition attacks (scans)
- Vulnerabilities: It is interesting to express the relationship between the attacks and vulnerabilities exploited in MANET; it will particularly help choose (phase test) attacks that exploit these vulnerabilities
- Means by which the attack is launched: It may be the network traffic, the action executed directly on the node
- Target: It can be divided into very specific objectives, such as the routing protocol, the node itself (e.g., food) and bandwidth power transmission channel

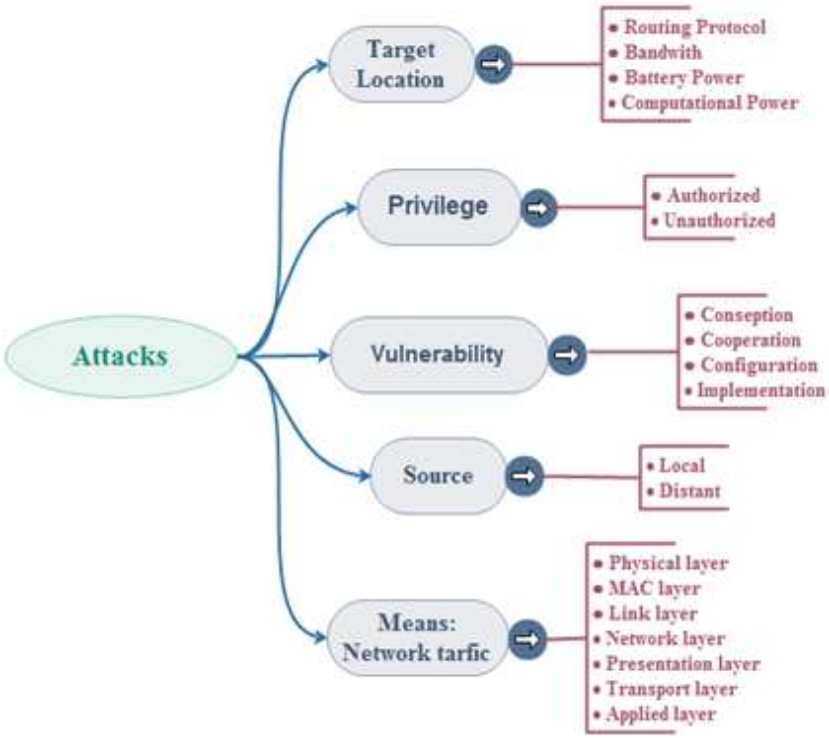

Fig. 1. Attack in MANETs: Classes and attributes

Fig. 2. Generation of test cases for Wormhole attack

Results and Discussion

Based on our proposed classification, we can generate all cases of possible attack test. The most appropriate method in this context is the Tree Classification Method (CTEM) that helps the automatic generation of attack test case. Classification Tree Method (CTM) are supervised classification tools that have been developed by (Grochtmann and Wegener, 1995) in the field of software engineering.

As its name suggests, this method graphically represents the partitions of the input field as a tree. This method allows complete verification of the test object. For efficient use, this method Classification Tree Editor CTE was developed. This is a syntax leading graphic editor that offers effective support determination of test cases with the method of classification tree.

By means of the CTM, the input domain of a test object is regarded under various aspects that are assessed to be relevant for the test. For each aspect, disjoint and complete classifications are formed. Classes resulting from these classifications may be further classified. The stepwise partition of the input domain by means of classifications is represented graphically in the form of a tree. Subsequently, test cases are formed by combining classes of different dimensions. To construct the test-cases, a grid is drawn below the tree. The columns of the grid result from vertical lines that correspond to the leaves of the classification tree. A tester can construct a test case by selecting a single child class of each top-level classification.

Each row of the grid indicates a distinct category of test case. However, not all test cases are legal or valid. Therefore, the tester should identify all valid test cases and eliminate invalid ones. This often could be done by applying the constraints stated explicitly or implicitly in system specifications. A major advantage of the classification-tree method is that it turns test case selection and generation into a systematic process and making it easy to handle.

Moreover, the systematic generation and analysis of test cases prevents the overlook that might occur for some areas of input. Thanks to its graphical representation, it allows the visualization of ideas and could be a good mean of communication between testers and developers. In order to generate the possible test cases we used a tool called Classification Tree Editor (CTE) which enables the automatic generation of test cases.

CTE tool allows the constraints application on the classification tree. This helps to further reduce, consolidate or rearrange test cases in order to retain only the most relevant for the current assessment.

More precisely, the CTE offers a simple and powerful formalism for constraints expression by combining some rules which include some sub-ones. Between brackets (under a predicting form), some connectors such as:

- and (*)
- or (+)
- no (NOT)

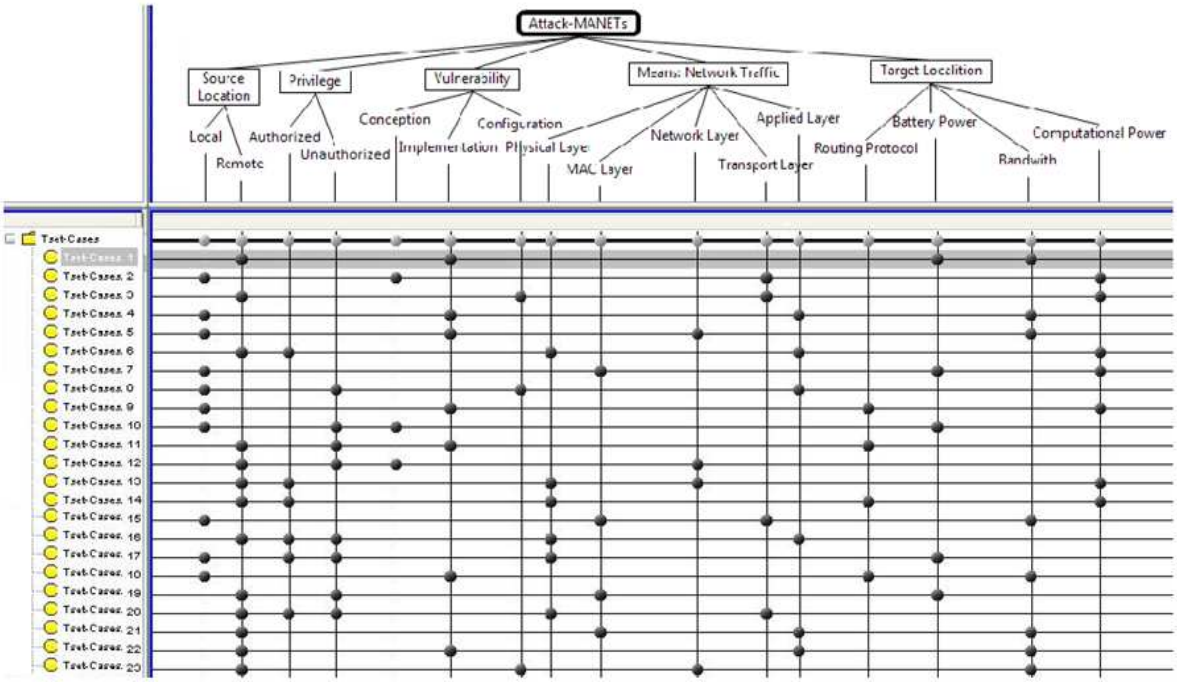

Fig. 3. Test cases produced by the CTE tool

For example, this test cases representing denial of service attacks (such as the "wormhole") is given by the following rule, this constraint generates 27 test-cases (Fig. 2):

- Source: Are launched locally or remotely
- Privileges provide Allowed access
- Vulnerabilities: Exploit vulnerabilities introduced during the cooperation
- Means: Are visible on the network at the network layer
- Target: Target routing protocols

This constraint generates test cases for local attacks that exploit the vulnerabilities introduced in the cooperation that provide "Allowed" access, which are visible on the network traffic and target routing protocols and formalized in our classification by the formula in (Fig. 3).

Conclusion

After studying the main classifications of attacks against ad hoc networks we proposed a new classification that works with the concept of class with the aim of improving the operation of IDS.

Applying the Classification Tree Method (CTM) to the new classification thus obtained and using the CTE tool, we were able to generate significant test cases and reduced in relation to other classifications.

This study presents two approaches for improving the evaluation process:

- A systematic method of generating test cases
- Selecting test cases based on an appropriate attacks classification.

Acknowledgement

The authors wish to thank anonymous reviewers for their valuable, insightful comments that improve the content of this review paper.

Funding Information

The authors have no support or funding to report.

Author's Contributions

The authors equally contributed in this work.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that the other author has read and approved the manuscript and no ethical issues involved.

References

Amit, M.H., N.S. Holkar and D. Nitnawwre, 2013. Investigatioin of application attack on MANET. Int. J. Comput. Applic., 71: 42-45. DOI: 10.5120/12430-9190

Awerbuch, B., D. Holmer, C. Nita-Rotaru and H. Rubens, 2002. An on-demand secure routing protocol resilient to byzantine failures. Proceedings of the 1st ACM Workshop on Wireless Security, Sept. 28-28, Atlanta, GA, USA, pp: 21-30. DOI: 10.1145/570681.570684

Gopalakrishnan, S. and P. Ganeshkumar, 2014. Intrusion detection in mobile ad hoc network using secure routing for attacker identification protocol. Am. J. Applied Sci., 11: 1391-1397. DOI: 10.3844/ajassp.2014.1391.1397

Grochtmann, M. and J. Wegener, 1995. Test case design using classification trees and the classification-tree editor cte. Proceedings of the 8th International Software Quality Week, (SQW' 95), San Francisco, USA, pp: 1-11.

Hansman, S. and R. Hunt, 2005. A taxonomy of network and computer attacks. Comput. Security, 24: 31-43. DOI: 10.1016/j.cose.2004.06.011

Mahdi, S.A., M. Othman, H. Ibrahim, J.M. Desa and J. Sulaiman, 2013. Protocols for secure routing and transmission in mobile ad hoc network: A review. J. Comput. Sci., 9: 607-619. DOI: 10.3844/jcssp.2013.607.619

Mamatha, G.S. and S.C. Sharma, 2010. Study of MANET: Network Layer attacks and defense mechanisms in MANETS-a survey. Int. J. Comput. Applic., 9: 12-17. DOI: 10.5120/1415-1911

Saber, M., B. Toumi, B. Abdelhamid and A. Mostafa, 2010. Amelioration of attack classifications for evaluating and testing intrusion detection system. J. Comput. Sci., 6: 716-722. DOI: 10.3844/jcssp.2010.716.722

Mpitziopoulos, A. and D. Gavalas, 2009. A survey on jamming attacks and countermeasures in WSNs. IEEE Commun. Surveys Tutorials, 11: 42-56. DOI: 10.1109/SURV.2009.090404

Murugan, R. and A. Shanmugam, 2010. A combined solution for routing and medium access control layer attacks in mobile ad hoc networks. J. Comput. Sci., 6: 1416-1423. DOI: 10.3844/jcssp.2010.1416.1423

Padmavathi, D.G. and M.D. Shanmugapriya, 2009. A survey of attacks, security mechanisms and challenges in wireless sensor networks. Int. J. Comput. Sci. Inform. Security, 4: 1-9.

Paulauskas, N. and E. Garsva, 2006. Computer system attack classification. Electron. Electr. Eng., 2: 84-87.

Pietro, R.D., S. Guarino, N.V. Verde and J. Domingo-Ferrer, 2014. Security in wireless ad-hoc networks-a survey. J. Comput. Commun., 51: 0140-3664. DOI: 10.1016/j.comcom.2014.06.003

Sen, S., J.A. Clarck and J.E. Tapiador, 2010. Security threats in mobile ad hoc networks. Security Self-Organizing Netw., 1: 127-145. DOI: 10.1201/EBK1439819197-9

Singh, R., P. Singh and M. Duhan, 2014. An effective implementation of security based algorithmic approach in mobile adhoc networks. Human-centric Comput. Inform. Sci., 4: 7-7. DOI: 10.1186/s13673-014-0007-9