11

A Survey on new Threats and Countermeasures on Emerging Networks

Jacques Saraydayran[1], Fatiha Benali[2] and Luc Paffumi[1]
[1]*LogLogic R&D*
[2]*INSA de Lyon*
France

1. Introduction

Companies business is more and more influenced by the rapid evolution of technologies. Indeed, companies mostly rely on computers for their business processes, for instance to keep tracks of stocks, to automate orders, and to store business secrets. From the electronic mail and web sites to the electronic commerce or online banking, all types of electronic services are widely used by everyone nowadays; very soon most of daily tasks will be done through the Internet. Many companies have become interdependent on their business, and dependent on each other infrastructures. New users have emerged such as mobile users (who can be employees, partners, customers). Therefore, access to computer systems is no longer physically limited.

Initially, computer systems were designed for environments and purposes completely different than today's ones. Indeed, a lot of systems were designed for small research labs where people worked in a trusted environment and thus had few need of authentication or encryption mechanism. An example of such a system is the Internet Protocol (IP). Even if those problems are known, it is often difficult to make changes in systems, in particular in those used by a great number of people around the world. Current systems still have vulnerabilities in design, implementation and configuration that may be used by outsiders to penetrate systems, or by legitimate users to misusing their privileges. New threats emerged with new vulnerabilities: increase in amount of anomalous and malicious traffic on the Internet, destructive worms, virus that spread quickly, large coordinated attacks against organizations such as distributed denial-of-service attacks, and even small attacks are very frequent due to free availability of attacking tools. Threats are increasing both in number, severity, sophistication and impact. Attacks can cause serious damages such as loss of income, time, intellectual property, reputation, sensitive information and a disruption of critical operations within an organization.

In this context, security has been raised to an important level due to increased threats, as well as legislation and compliance requirements. The security is become necessary to protect our vulnerable society. First attentions were focused on protecting information systems and data from accidental or intentional unauthorized accesses, disclosure, modification, or destruction. The consequences of these mechanisms can range from degraded or disrupted service to customers to corporate failure. Today, traditional security mechanisms cannot completely address those threats and need to be improved with new intrusion detection mechanisms.

Intrusion detection covers both methods and tools to detect intrusions performed by both outsiders and insiders.
In various contexts such military communication services, on-demand service on mobile computer/PDA, emergence disaster coordinating efforts, the apparition of new needs highlights weaknesses of standard network architectures. New emerging networks grew up aiming at providing network communication between distributed mobile transmitters (probes, computer, mobile phone, PDA). Such networks, called Mobile Ad-hoc NETworks (MANET) consist of autonomous systems that are composed of a variety of mobile hosts. These hosts form a temporary network without any fixed architecture. A MANET provides new characteristics such as dynamic topology without any fixed architecture and entails some constraints (limited resources and physical architecture).
The success of the MANET networks increases due to its properties and new available services. Nevertheless, the success of such a network was followed by the emergence of a large amount of new threats. The characteristics of MANET networks imply new weaknesses and vulnerabilities. For example, the routing protocol is one of the most sensitive parts of a MANET network. Due to its configuration, the establishment of the network topology and the routing service is built through nodes collaboration. This collaboration is an opportunity for malicious nodes and attackers.
This chapter provides a survey of recent threats and attacks existing on MANET networks. In a first part, we will provide a description of new threats coming from on demand services and applications. This description include the presentation of attack classifications in the intrusion detection field and select some that fit with MANETs requirements. To counter such attacks, security mechanisms based on node collaboration and reputation are discussed and compared in a second part. Finally, the MANET threats and security are discussed in a last part.

2. Attacks and security breaches on MANET

As information systems become more and more important to our everyday lives, it is necessary to protect them from being compromised. In the information systems context, intrusions refer to any unauthorized access or malicious use of information resources.

2.1 General attacks

There are numerous network-based attacks that can be found in both wired and wireless network, this first part sums up the main ones.

- **I**P Spoofing
  The attacker uses the IP address of another machine to be ”hidden” and exploit weak authentication methods. If the target machines rely on the IP address to authenticate (e.g. source IP address access lists), IP spoofing can give an attacker access to systems he should not have access to. Additionally, IP spoofing can make it very difficult to apprehend an attacker because logs will contain decoy addresses instead of real ones.
- **S**ession hijack
  The attack consists in stealing network connections by kicking off the legitimate user or sharing a login. This type of attack is used against services with persistent login sessions, such as Telnet, rlogin, or FTP. For any of these services, an attacker can hijack a session and cause a great amount of damage. The connection between two hosts is monitored to observe the TCP sequence number of the packet. The attacker guesses the appropriate

sequence numbers and spoofs one of the participants address, taking over the conversation with the other participant.

- **D**enial-of-service (DoS)
  DoS attacks are among the most common exploits available today. As their name implies, a denial-of-service attack prevents (legitimate) users from being able to use a service. By bringing down critical servers, these attacks could also present a real physical threat to life. An attacker can cause the denial of service by flooding a system with bogus traffic. The technical result of a denial of service can range from applications sending wrong results to machines being down. Malformed Packet Attacks can be used to make DoS by generated badly formatted packets. Many vendor product implementations do not take into account all variations of user entries or packet types. If the software handles such errors poorly, the system may crash when receiving such packets. A classic example of this type of attack involves sending IP fragments to a system that overlap with each other. Some unpatched Windows and Linux systems will crash when they encounter such packets.
- **B**uffer overflow
  Buffer overflows attacks consists in injecting data into a program (e.g. in web page form) to run malicious code. They can be used by an attacker to take control of a remote system or by local malicious users to elevate their privileges. This exploits weak parameters verifications. If user input length is not examined by the code, a particular variable on the stack may exceed the memory allocated to it on the stack, overwriting all variables and even the return address for where execution should resume after the function is complete. Therefore, with very carefully constructed code, the attacker can actually enter information as a user into a program that consists of executable code and a new return address. Such attack allows an attacker to break out of the application code, and access any system components with the permissions of the broken program. If the broken program is running with superuser privileges, the attacker has taken over the machine with a buffer overflow.

2.2 Attacks on MANET

Security problematics on wired networks have been deeply studied. Many MANETs characteristics make it harder to secure such environment and new threats appeared on such networks. Those characteristics can be classified into 3 categories:

- Hardware: Node mobility, wireless medium, resources consumption,
- Communication: Distributed administration, variable topology,
- Software: On demand service, Reputation based applications.

Such MANET-specific attributes entails the appearance of new attacks that were classified and described in different papers. The following section describes the most know attacks. Due to the need of cooperation for network topology building, communication and services, distribution, new types of threats appears on MANET.

2.2.1 Hardware MANET attacks

One of the main MANETs properties is the wireless communication mode. Such communication mode has the advantage to allow network components to move easily without losing connection. Nevertheless wireless communications and mobility are very exposed to the following attacks.

- Eavesdropping
  This attack consists in sniffing the wireless medium to collect messages exchanged between

different nodes. This is a very simple attack as the wireless medium is shared by everyone in the MANET. If no cipher mechanism is used, the attacker can directly have access to the information exchanged. In case ciphering is used, many techniques allow attacker to uncipher weakly encrypted messages.

- Physical access to mobile components
  Mobile devices are smaller and smaller and are widely transported. Unlike laptops, PDAs and mobile phones (smartphones) are seldom securely locked and/or ciphered. If they are stolen, the attacker can, most of the time, easily take control of the device and steal information. In the worst cases, the attacker can enter a MANET thanks to the credentials left in the device.

- Wireless communication DoS
  Due to the wireless characteristics, all nodes belonging to a MANET receive all messages exchanged within their range. By injecting a huge amount of traffic close to the different machines, a denial of service can be triggered. Nodes having few computing capabilities will not be able to handle all traffic and could either crash or miss important messages.

- Signal jamming
  An attacker injects in the wireless medium some noise. The increased noise floor entails a degraded signal-to-noise ratio which prevents legitimate users to handle messages correctly.

2.2.2 Protocol MANET attacks

These types of attacks mainly target the routing features (discovery, forwarding, etc.) of the different nodes in the network. As there is no ”routers” (devices dedicated to routing) in MANETs, the routing mechanisms are one of the most critical services of the MANETs.

- Wormhole attack Ilyas & Dorf (2003)
  This attack consists in collecting packets in a part of the MANET and sending them to another location, which generates a ”tunnel”. This latter is referred to as a wormhole. Legitimate nodes will miss information. This can especially generate wrong routing tables (if the original destination node does not receive updated routing information) on different nodes (see blackhole attack) or redirection of useful information to illegitimate users.

- Blackhole attack Baadache & Belmehdi (2010)
  In this attack, the attacker drops some of the received messages that should be forwarded. In a first step, the malicious node gives wrong routes to its neighbors. By doing this, legitimate nodes will send messages to malicious nodes that will drop all or part of the messages. Most of the time, only part of the messages is not forwarded to avoid suspicion of neighbors (that could monitor the traffic).

- Byzantine attack Awerbuch et al. (2002)
  Such an attack represents an attacker aiming at disturbing the overall network communication. The malicious node generates wrong routing information to create, for instance, loops, wrong paths which entail delays or packet drops.

- Routing table poisoning
  A malicious node sends erroneous routing updates to legitimate nodes or modifies correct route update packets. The legitimate nodes then use non-optimal routes and/or can generate network congestion.

- Routing table overflow
  Legitimate nodes in the network are sent route updates to non-existing nodes in order to generate an overflow of the routing tables and prevent the creation of entries corresponding to new routes to correct nodes. This attack is more effective on proactive routing protocols than on reactive ones.
- Malicious broken-links report
  The malicious nodes inform legitimate users that some links are broken whereas they are not. This attack affects route maintaining protocols or route discovering protocols.
- Rushing attack Hu et al. (2003b)
  Two malicious nodes take advantage of the tunnel generated by a wormhole attack. In certain cases, the ″tunneled″ packets will reach the destination before the normal route. Such a result characterizes the rushing attack.
- Resource consumption attack
  Malicious nodes inject wrong and extra information in the network. Such actions reduce the bandwidth available for ″normal″ activities and make them perform extra (unnecessary) actions. Consequently, that makes local resources (such as battery) decreasing quickly.
- Location disclosure attack
  This is a kind of information leak attack. Attackers gather information regarding the network topology (locations, routing information, etc.). This information is then used to build attack scenarios.

2.2.3 Software MANET attacks

On MANET nodes are most of the time resource limited. To reach some services, nodes need to ask service to neighbors. Such mechanisms are mainly based on node reputation for the service provider selection.

- Application proving fishing
  One of the characteristics of MANETs is their decentralized architecture. Applications can be run by any node on the network. The benefit of such architecture is its resilience to failures. However, a malicious node can take advantage and run fake applications. It then sends messages to their neighbors indicating that they run the application. Combined with previously presented attacks (e.g. wormhole), the malicious node can prevent other nodes to be aware of the correct location of the legitimate application and avoid any suspicion,
- Reputation Attack
  In some MANETs, in order to prevent the previous type of attacks, a trust mechanism has been designed: each node assigns a trust level to the other nodes of the network. This level is based on their direct and indirect relationships. By degrading the other legitimate nodes trust level, a malicious node can create a denial of service and/or a denial of participation in all or part of the communications. This is called a repudiation attack.

2.3 Attacks classification

Security countermeasures which are going to provide the essential tools to develop security defenses and improve the overall security outcomes, require a deep understanding of the threats. The overall tools used to protect the IS emphasize the complexity of collaborating all these tools and mapping the security threats through classification categories. Managing information security has to deal with the heterogeneity of data generated by the monitoring products. In follows, we discuss several research works that classify security threats.

There is a high number of attack classifications proposed in intrusion detection research. Four approaches were used to describe attacks: list of terms, taxonomies, ontologies and attacks language. The easiest classification is a list of single terms Cohen (1997), covering various aspects of attacks, the number of terms differs from author to author. Other authors have created categories to group many terms under a common definition. Cheswick and Bellovin classify attacks into seven categories Cheswick & Bellovin (1994). Stallings classification Stallings (1995) is based on the action, the model focuses on transiting data and defines four categories of attacks: interruption, interception, modification and fabrication. Cohen Cohen (1995) groups attacks into categories that describe the result of an attack. Some works developed categories based on empirical data, each one uses an events corpus generated in a specific environment. Neumann and Parker Neumann & Parker (1989) works were based on a corpus of 3000 incidents collected for 20 years; they created nine classes according to attacking techniques. Terms tend not to be mutually exclusive; this type of classification cannot provide a classification scheme that avoids ambiguity.

To avoid these drawbacks, a lot of taxonomies were developed to describe attacks. Neumann Neumann (1994) extended the classification in Neumann & Parker (1989) by adding the exploited vulnerabilities and the impact of the attack. Lindqvist and Jonson Lindqvist & Jonsson (1997) presented a classification based on the Neumann classification Neumann & Parker (1989). They proposed *intrusion results* and *intrusion techniques* as dimensions for classification. John Howard presented in Howard (April 1997) a process-driven taxonomy of computer and network attacks in five dimensions: *attackers, tools, access, results* and *objectives*. John Howard worked on the incidents of the Computer Emergency Response Team (CERT). Howard extends this work in Howard & Longstaff (1998) by refining some of the dimensions. Representing attacks by taxonomies is an improvement compared with the list of terms: individual attacks are described with an enriched semantics, but taxonomies fail to meet mutual exclusion requirements, some of the categories may overlap. However, the ambiguity problem still exists with the refined taxonomy.

Undercoffer and al Undercoffer et al. (2003) describe attacks by an ontology. It is a new effort for describing attacks in intrusion detection field by sharing the knowledge about intrusions in distributed IDS environment. Initially, they developed a taxonomy defined by *the target, means, consequences of an attack* and *the attacker*. The taxonomy was extended to an ontology, by defining the various classes, their attributes and their relations based on an examination of 4000 alerts. The authors have built correlation decisions based on the knowledge that exists in the modeling. The developed ontology represents the data model for the triggered information by IDSs.

Attack languages are proposed by several authors to detect intrusions. These languages are used to describe the presence of attacks in a suitable format. These languages are classified into six distinct categories Eckmann et al. (2002): *Exploit languages, event languages, detection languages, correlation languages, reporting languages* and *response languages*. The correlation languages are currently the interest of several researchers in the intrusion detection community. They specify relations between attacks to identify numerous attacks against the system. These languages have different characteristics but are suitable for intrusion detection in a particular environment. Language models are based on the models that are used for describing alerts or events semantics. They do not model the semantics of events but they implicitly use taxonomies of attacks in their modeling.

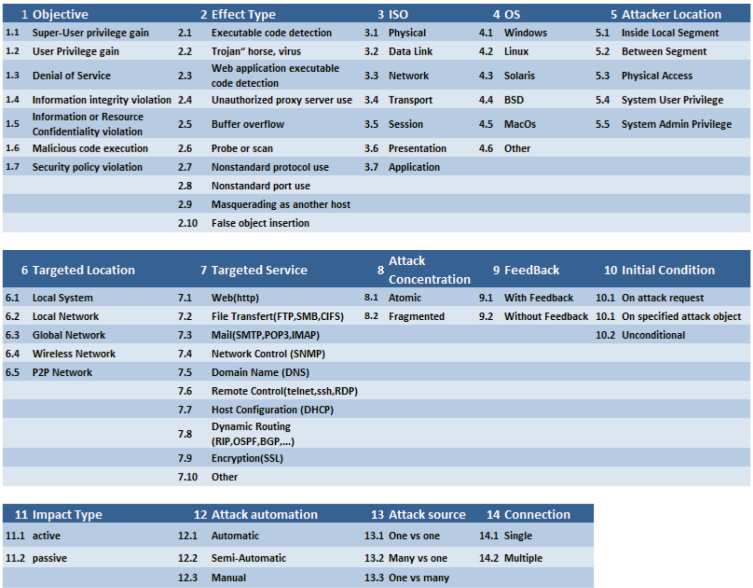
All the researches quoted above only give a partial vision of the monitored system, they were focused on the conceptualization of attacks or incidents, which is due to the consideration of

a single type of monitoring product, the IDS.
It is important to mention the efforts done to realize a data model for information security. The first attempts were undertaken by the American agency - Defense Advanced Research Projects Agency (DARPA), which has created the Common Intrusion Detection Framework (CIDF) Staniford-Chen & Schnackenberg (1998). The objective of the CIDF is to develop protocols and applications so that intrusion detection research projects can share information. Work on CIDF was stopped in 1999 and this format was not implemented by any product. Some ideas introduced in the CIDF have encouraged the creation of a work group called Intrusion Detection Working Group (IDWG) at Internet Engineering Task Force (IETF) co-directed by the former coordinators of CIDF. IETF have proposed the Intrusion Detection Message Exchange Format (IDMEF) Curry & Debar (2007) as a way to set a standard representation for intrusion alerts. The effort of the IDMEF is centered on alert syntax representation. In the implementations of IDSs, each IDS chooses the name of the attack, different IDSs can give different names to the same attack. As a result, similar information can be tagged differently and handled as two different alerts (IDMEF became a standard format with the RFC 4765 Curry & Debar (2007)).
There is no previous work reported in the literature about specific attack classifications in Wireless Sensor Networks (WSN). Partial solutions exist that allows checking the security of the WSN against a some type of attacks Perrig et al. (2002). Recent work in Padmavathi & Shanmugapriya (2009) have classified attacks basically into two categories; active attacks and passive attacks. Under each category, a list of attacks and their definition that widely happen on WSN are presented. No classification scheme or rule were presented to avoid ambiguity.
Even if it is not specific to MANETs, an interesting attack classification was proposed in Paulauskas & Garsva (2006). Authors suggest to characterize attacks around 14 attributes: the objective of the attack(1), the effect type produce by the attack(2), the OSI layer involved (3), the targeted Operating System (4), the location of the attacker (5), the attacker target location (6) and the attacked service (7), attack concentration (8) (e.g. target one packet or several packets), need of feedback (9) (e.g. sniffing attack do not need feedback), the initial attack conditions (10), the impact type (11), the number of attack sources (13) and connection quantity (14) (figure 1). Detailing number of attack parameters, this approach is an effective way to classify and define attacks.

2.4 MANET attacks classification mapping

As presented in the previous section, MANETs, in a security point of view, are very interesting and offer various challenges. Not only are they vulnerable to generic threats but as well to wireless specific ones. To better understand them and find the best solutions to faces those attacks, classifications - presented above - were used. The attack classification of Paulauskas & Garsva (2006) allows clearly defining attacks and classifying them. We propose to map the 14 features defined in their paper with the MANET attacks defined in 2.2 (figure 2).
First of all, all MANET attacks share common features:

- *Target Location* (6): in MANET each node collaborates with unknown node to build a network. Each targeted object is located on individual node. Despite the entire network could be affected the target object is still located on locate system (6.1) for each participant.
- *Attack Execution Initial Condition* (10): all described attacks are focused on ad hoc network. The initial condition for these attacks is that the targeted object (10.1) runs dynamic ad hoc routing protocol and wireless communications.
- *Connection quantity* (14): described attacks always used single connection (14.1) attack type.



1	Objective	2	Effect Type	3	ISO	4	OS	5	Attacker Location
1.1	Super-User privilege gain	2.1	Executable code detection	3.1	Physical	4.1	Windows	5.1	Inside Local Segment
1.2	User Privilege gain	2.2	Trojan“ horse, virus	3.2	Data Link	4.2	Linux	5.2	Between Segment
1.3	Denial of Service	2.3	Web application executable code detection	3.3	Network	4.3	Solaris	5.3	Physical Access
1.4	Information integrity violation	2.4	Unauthorized proxy server use	3.4	Transport	4.4	BSD	5.4	System User Privilege
1.5	Information or Resource Confidentiality violation	2.5	Buffer overflow	3.5	Session	4.5	MacOs	5.5	System Admin Privilege
1.6	Malicious code execution	2.6	Probe or scan	3.6	Presentation	4.6	Other		
1.7	Security policy violation	2.7	Nonstandard protocol use	3.7	Application				
		2.8	Nonstandard port use						
		2.9	Masquerading as another host						
		2.10	False object insertion						

6	Targeted Location	7	Targeted Service	8	Attack Concentration	9	FeedBack	10	Initial Condition
6.1	Local System	7.1	Web(http)	8.1	Atomic	9.1	With Feedback	10.1	On attack request
6.2	Local Network	7.2	File Transfert(FTP,SMB,CIFS)	8.2	Fragmented	9.2	Without Feedback	10.1	On specified attack object
6.3	Global Network	7.3	Mail(SMTP,POP3,IMAP)					10.2	Unconditional
6.4	Wireless Network	7.4	Network Control (SNMP)						
6.5	P2P Network	7.5	Domain Name (DNS)						
		7.6	Remote Control(telnet,ssh,RDP)						
		7.7	Host Configuration (DHCP)						
		7.8	Dynamic Routing (RIP,OSPF,BGP,...)						
		7.9	Encryption(SSL)						
		7.10	Other						

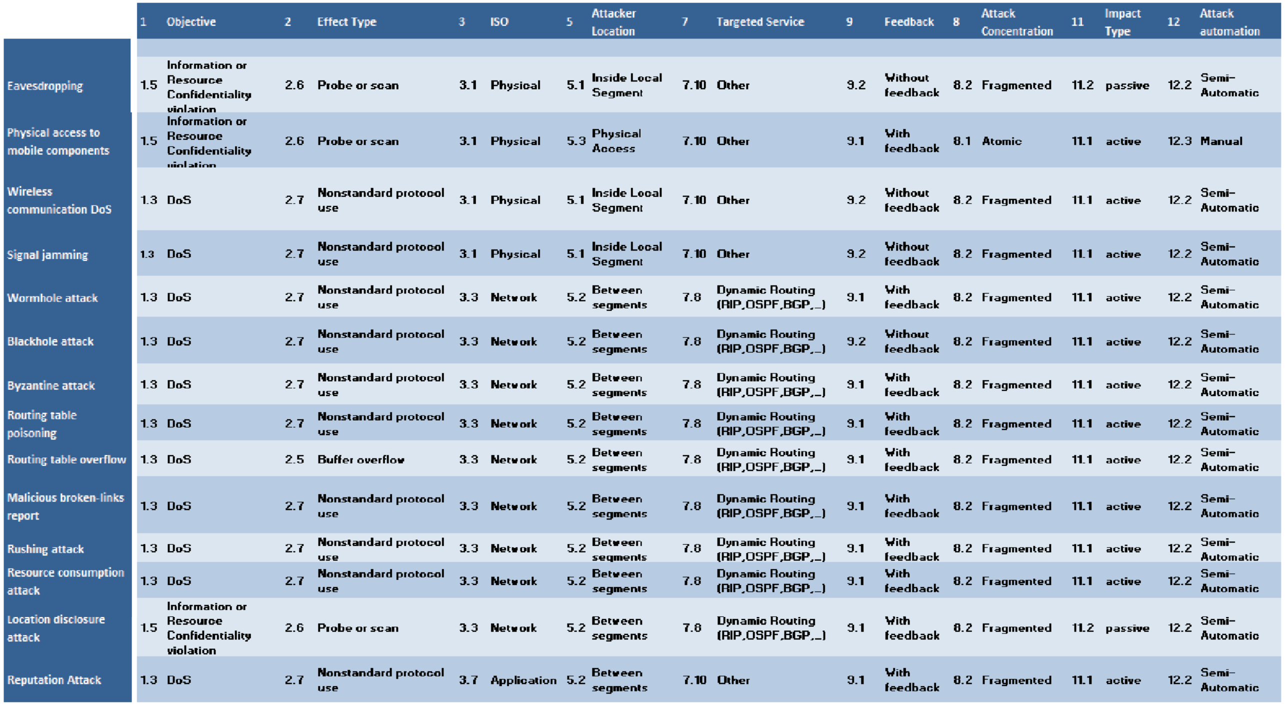
11	Impact Type	12	Attack automation	13	Attack source	14	Connection
11.1	active	12.1	Automatic	13.1	One vs one	14.1	Single
11.2	passive	12.2	Semi-Automatic	13.2	Many vs one	14.2	Multiple
		12.3	Manual	13.3	One vs many		

Fig. 1. Attack Taxonomy Paulauskas & Garsva (2006)

The feature *Operating System* (4) is not mandatory for MANET attack. In fact all attacks depend on the specifics routing protocol and not a specific Operating System.
The attack objective of MANET attacks are mostly focused on the *DoS* (1.3) on the routing protocol and produce a *non standard protocol use* (2.7). Some others attacks (Eavesdropping,Physical access to mobile components,Location disclosure attack) attempt to gathering information (1.5) working as *probe or scan* (2.6).
Three types of ISO layers are targeted:

- The *Physical* (3.1) layer inducing two types of attacker location: a *Physical Access* (5.3) to the MANET component itself and *Inside Local Segments* (5.2) location meaning that attacker is in the radio range of the targeted component,
- The *Network* layer (3.3) implying that the attacker is at least *Between Segments* (5.2),
- The *Application* layer (3.7) concerning the Reputation attack.

Targeted Service mainly differs from hardware attack to protocol attacks. Protocol attacks target the collaborative *routing service* (7.8) whereas Hardware attack disturbs physical communication or physically access to data (*other* 7.10). Software attack differs also from Protocol attacks by targeted ”‘service provider”’ mechanism (*other* 7.10).
Finally, all considered attacks are active by interacting directly with the MANET components (*active* 11.1). Only Eavesdropping and Location disclosure use only received information (*passive* 11.2). MANET attacks are complex and need to exchange several information to produce the expected effect (attack *fragmented* 8.2 except Physical Access). With the help of context aware definition MANET attacks could be automated(*Semi-Automatic* 12.2). Only the Physical Access attacks involve manual actions of the attacker.



	1	Objective	2	Effect Type	3	ISO	5	Attacker Location	7	Targeted Service	9	Feedback	8	Attack Concentration	11	Impact Type	12	Attack automation
Eavesdropping	1.5	Information or Resource Confidentiality violation	2.6	Probe or scan	3.1	Physical	5.1	Inside Local Segment	7.10	Other	9.2	Without feedback	8.2	Fragmented	11.2	passive	12.2	Semi-Automatic
Physical access to mobile components	1.5	Information or Resource Confidentiality violation	2.6	Probe or scan	3.1	Physical	5.3	Physical Access	7.10	Other	9.1	With feedback	8.1	Atomic	11.1	active	12.3	Manual
Wireless communication DoS	1.3	DoS	2.7	Nonstandard protocol use	3.1	Physical	5.1	Inside Local Segment	7.10	Other	9.2	Without feedback	8.2	Fragmented	11.1	active	12.2	Semi-Automatic
Signal jamming	1.3	DoS	2.7	Nonstandard protocol use	3.1	Physical	5.1	Inside Local Segment	7.10	Other	9.2	Without feedback	8.2	Fragmented	11.1	active	12.2	Semi-Automatic
Wormhole attack	1.3	DoS	2.7	Nonstandard protocol use	3.3	Network	5.2	Between segments	7.8	Dynamic Routing (RIP,OSPF,BGP,..)	9.1	With feedback	8.2	Fragmented	11.1	active	12.2	Semi-Automatic
Blackhole attack	1.3	DoS	2.7	Nonstandard protocol use	3.3	Network	5.2	Between segments	7.8	Dynamic Routing (RIP,OSPF,BGP,..)	9.2	Without feedback	8.2	Fragmented	11.1	active	12.2	Semi-Automatic
Byzantine attack	1.3	DoS	2.7	Nonstandard protocol use	3.3	Network	5.2	Between segments	7.8	Dynamic Routing (RIP,OSPF,BGP,..)	9.1	With feedback	8.2	Fragmented	11.1	active	12.2	Semi-Automatic
Routing table poisoning	1.3	DoS	2.7	Nonstandard protocol use	3.3	Network	5.2	Between segments	7.8	Dynamic Routing (RIP,OSPF,BGP,..)	9.1	With feedback	8.2	Fragmented	11.1	active	12.2	Semi-Automatic
Routing table overflow	1.3	DoS	2.5	Buffer overflow	3.3	Network	5.2	Between segments	7.8	Dynamic Routing (RIP,OSPF,BGP,..)	9.1	With feedback	8.2	Fragmented	11.1	active	12.2	Semi-Automatic
Malicious broken-links report	1.3	DoS	2.7	Nonstandard protocol use	3.3	Network	5.2	Between segments	7.8	Dynamic Routing (RIP,OSPF,BGP,..)	9.1	With feedback	8.2	Fragmented	11.1	active	12.2	Semi-Automatic
Rushing attack	1.3	DoS	2.7	Nonstandard protocol use	3.3	Network	5.2	Between segments	7.8	Dynamic Routing (RIP,OSPF,BGP,..)	9.1	With feedback	8.2	Fragmented	11.1	active	12.2	Semi-Automatic
Resource consumption attack	1.3	DoS	2.7	Nonstandard protocol use	3.3	Network	5.2	Between segments	7.8	Dynamic Routing (RIP,OSPF,BGP,..)	9.1	With feedback	8.2	Fragmented	11.1	active	12.2	Semi-Automatic
Location disclosure attack	1.5	Information or Resource Confidentiality violation	2.6	Probe or scan	3.3	Network	5.2	Between segments	7.8	Dynamic Routing (RIP,OSPF,BGP,..)	9.1	With feedback	8.2	Fragmented	11.2	passive	12.2	Semi-Automatic
Reputation Attack	1.3	DoS	2.7	Nonstandard protocol use	3.7	Application	5.2	Between segments	7.10	Other	9.1	With feedback	8.2	Fragmented	11.1	active	12.2	Semi-Automatic

Fig. 2. MANET Attack Taxonomy Mapping

3. Countermeasure and security achievements on MANET

The section 2.2 describes and defines attack opportunity on MANET. Despite lots of attack vectors on wireless communications, collaborative routing protocol and collaborative services providing, emerging security solutions and protocols exist and preserve MANET from such threads. In this section, the different counter measures mechanisms are presented and compared allowing showing the current available thread countermeasures.

3.1 Security challenges

Securing company data, activities and communications become an open challenge and especially nowadays where collaboration and on demand services grow up. As introduced in 1, the appearance of new needs involved the emergence of new vulnerabilities and cyber criminality organizations. The first step to deal with this threat is to understand what security means in our company/organization context. All risk management procedures (*COBIT* (2007),*ISO 27000 series* (2005)]) are organized around the following fundamental security indicators Bing Wu (2006):

- **Confidentiality** is to keep information available only for authorized entities (users, applications, nodes). All unauthorized entities cannot read, manipulate, execute or gather information coming from the system. E.g. invoices can only be read by users of the sales/accounting entity.
- **Integrity** ensures that transmitted/stored/used information is not altered or destroyed by any illegal manipulation. E.g. an email sent is not modified until it reaches its destination.
- **Availability** ensures that services can be used at any moment and provide the expected results. Any service (application, networks, hardware) is kept available to legitimate entities. Most of the time, DoS attacks target availability of systems.
- **Accountability** ensures that any entity that performs an action can be made responsible for its actions. This entails the use of authentication mechanisms. Access control allowing only authorized users, network flows or packets can be viewed as a sub-property of authentication.
- **Non-repudiation** defines the fact that entities making an action cannot claim that they did not perform this action. E.g. a user who digitally signed an email cannot deny that he has not sent this email.

3.2 Countermeasure and security tools definition

Countermeasures, which can be procedures and security tools, aim at ensuring that one or several Security Indicators linked to an object are preserved. To define a security tool we will address the following six questions:

- **Why** is the security tool used for? Which type of security indicators is targeted by the security tool?
- **What** types of services are protected by the security tool?
- **When** is the security tool active? When does the security tool operate to reach its objective?
- **Where** is the security tool active? What is the monitoring perimeter?
- **Who** is responsible for the security tool? What is his objective?
- **How** does the security tool work to reach its objective?

Several security tool properties have been described in literature to classify those tools in different families (Debar et al. (1999)). In this section, we propose a set of attributes responding to the questions listed above. They are firstly presented and then described. The security indicators are used to define the **Why** attribute. The **What** is defined by the OSI Layer attribute defining the targeted services. The **When** question is covered by the Time Frame attribute. The Scope attribute (area monitored by the tool) defines the **Where**. The person responsible for the the security tool (**Who**) is expressed in the Security tools attribute called purpose. Finally the Internal Architecture attribute determines the **How**.

- **OSI Layer** : Several approaches classified security breaches and attacks Paulauskas & Garsva (2006). ISO layer appears as a starting point to know which service is protected by the security tool. This attribute ”localizes” the action of the security tool. The Open System Interconnection (OSI) layer ISO-IEC (1994) is composed of the well known seven layers:
  - Physical layer is composed of all hardware or physical processes. This layer defined the electrical and physical specifications for devices. Physical layer security tools can be biometrics door mechanisms, digital lock as well as channel radio selection.
  - Data Link layer aims at providing communication with direct neighbor in Wan network or in nodes on a same segment in LAN. Intrusion Detection system monitoring ARP address and preventing ARP attack or MAC address spoofing securing the Data link Layer.
  - Network is responsible for all data transition between network segments inside a LAN/MAN/WAN. This layer aims at defining packet path and network topology. Varieties of security tools operating at this level. Tools like Intrusion Detection System, Secure routing protocol or virtual Private Network can be quoted.
  - Transport layer manages end-to-end communication. This is the upper layer where error correction is managed. Transport Layer Security protocol (RFC 2246) is one of the most important ways to secure the transport layer.
  - Session layer aims at synchronizing communications and managing transactions. This consists, for instance, in correcting errors by restoring past known states.
  - Presentation layer ensures the application data encoding. This layer converts data between manipulated applicative data and byte chain forwarded by the network.
  - Application layer manages all communications and data of applications and services. Most of security tools cover the session, the presentation and the application layers. Anti-viruses are well known security tools ensuring the good behavior of applications.
- **Protect purpose** : the security indicators (Confidentiality, Integrity, Availability, Accountability, Non-repudiation) that should be ensured but the security tools are referred to as protect purpose.
- **Scope** : Security tools operate at different locations of the Information System. Four perimeters have been identified from the Host (specific coverage) to the Whole System (extended coverage).
  - Single Component : security tools aims at protecting a single host. Antiviruses or personal Firewalls focus their work on single network components.

  - Network Area: security tools protect components of a delimited network zone. Located on network segments, Network Intrusion Detection Systems are especially designed to detect malicious network activities. Firewalls become also key security points in the protection of LANs or DeMilitarized Zones (DMZ).
  - Overall IS: the security tool intends to protect the entire company or organism Information System. We can quote Distributed IDS, protecting all IS components or Public Key Infrastructure allowing communication privacy in the IS.
  - Communication: security tools aiming at ensuring a security indicator such as confidentiality or availability are often embedded inside communication protocol. Secure Routing protocol (ad hoc secure routing protocol) ensuring the whole system secure behavior is an example.
- **Purpose** : Bing Wu (2006) defines two families of security tools classified according to their manager's purposes.
  - Preventive: all security tools aiming at avoiding attacks or malicious activities by assuring authentication or encryption form the first line of defense in the IS. Cryptographic protocols, secure routing protocols, physical authentication mechanisms (PIN code) are examples of such preventive mechanisms.
  - Reactive security tools form the second line of defense ensuring the detection and reaction against attacks. IDS, antiviruses are part of this second line of defense.
- **Internal Architecture** defines how the tool's modules work and its behavior. It also specifies the internal communication.
  - Standalone architecture means that the security tool is isolated and makes decision alone. Configuration files and security policies are directly loaded on a single component. Most of firewalls are classified in this category using its own knowledge of the environment.
  - Central architecture defines security tool collecting information through probes and making decisions on a central computation point. Security Event Management systems (LogLogic SEM, Prelude) use distributed agents to collect information. The set of data are then analyzed on a central component.
  - Hierarchical architecture describes security tool that uses distributed components. Each component holds an analysis function block aims at making a local decision (Zheng Zhang & Ucles (2001), S. Staniford-Chen & Zerkle (1996)). Several levels can be implemented, each one managing the lower level.
  - Collaborative architecture provides communication between distributed security components. Decision is not computed on a central component but coming from the exchanged experience between each security component. Such architecture allows achieving a Security objective with the help of the others entities. Local decision is improved with the enrichment neighbors information and global decision can be made to improve the global system security Martin Rehak (2008).
  - Protocol architecture defines security tools embedded in global system behavior. The success of such system is based on predefined policy respected by each component in the network. PKI architectures hold cryptographic rules and best practices. Any entity wanting to benefit from such security mechanism needs to respect protocol to be able to exchange information.

- **Time frame** attribute is used to identify the security tool protection period. It describes when the security tool operates.
  - Real-Time processes are running all the time by, they do not have to be triggered to be active. Mechanisms such as encryption are a good example.
  - On demand processes are only called whenever they are needed. For instance, forensics T. Duval & Roger (2004), vulnerability scanners (Nessus, Qualys) and backup systems are on demand systems.

3.3 Security tools parameters representation

To easily compare Security tools, we provide a security tool parameters graphical representation allowing to link parameters together. Two different panels are used. The first panel represents a list of protection purposes. This list displays an overview of the security indicators covered by presented security tools. A second panel is composed of a radar chart representing the other security parameters defined in section 3.2. The parameters are organized as follow.

On the left part of the graph, the Time Frame and Purpose parameters are listed. This side of the graph represents the reactivity of the security tools. Real-time (Time Frame) and reactive (Purpose) security tools parameters are more reactive than on-demand (Time Frame) and preventive (Purpose) security tool.

On the right part of the graph, the scope and internal architecture parameters expresses the global coverage of the security tool. Communication (Scope) and protocol (Internal Architecture) security tool parameter have got a wider coverage than Single component (scope) and standalone (Internal Architecture).

The top branch is the layer parameter. This parameter is transversal to the others.

3.4 Security tool attributes allocates: samples

This section shows how the Security tools parameters representation allows comparing different security tools. We will take as examples a Certificate and a Firewall.

3.4.1 Certificate security tool

Certificates are built to prove the Identity of its owner. Different objects are held by the certificate such as user or component identities (Name, Group,...), public key of the certificate owner, digital signature of the Certificate Authority (CA) who delivered the certificate. Certificate can be used to ensuring the authentication its owner, using the asymmetric encryption mechanism certificate can guaranty non-repudiation and integrity of messages sent (digital signature of the owner), confidentiality of exchanges (encryption with public key). The certificate is defined by the following attributes:

- Layer (What): Application layer, PKI guaranties confidentiality, integrity, non-repudiation from the network communication to the application used. In case of the sending an email, digital signature, ensures the integrity of the message sent during the computation of the mail application, the ”transformation” of the presentation/session layer and during the message transport (transport/network/data Link/Physical layers).
- Protect Purpose (Why): Confidentiality, Integrity, Authentication and Non-Repudiation.
- Time Frame (When): On-Demand, the certificate properties used would be done on the demand of the application.

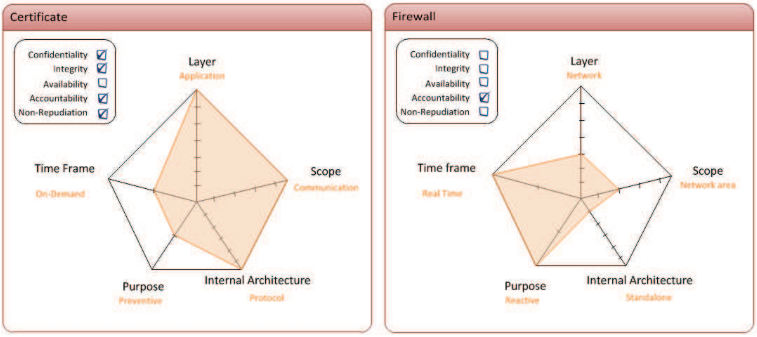


Fig. 3. Firewall Security Attribute Definition

- Scope (Where): Overall IS, the application of the certificate properties are available on the all the Information System.
- Purpose (Who): Preventive System, the security indicators covers by certificate prevents information from information disclosure and unauthorized modifications.
- Internal Architecture (How): Protocol, the deployment of certificates is realized via a Public Key Infrastructure. Any used components of the Information System needs to know How certificates and asymmetric encryption work to apply the security properties.

3.4.2 Firewall security tool

Firewall system aims at blocking all unauthorized network flows both from public network to the internal system and from internal system to the public network. the firewall is defined by the following attributes (figure 3)

- Layer (What): Network, Firewalls operated at the network level by analyzing network flows and apply authorized flows rules. Some firewalls operate at higher levels acting like proxies.
- Protect Purpose (Why): Authentication, Firewall guaranties an access control of the incoming network traffic.
- Time Frame (When): Real time, each incoming network flow is analyzed and dropped if needed.
- Scope (Where): Network area, Firewall guaranties the protection of defined networks area. In case of a company composed of several sites, several firewalls would be used, each one to protect one site.
- Purpose (Who): Reactive, the firewall allows blocking unauthorized communication by dropping network packet.
- Internal Architecture (How): Standalone, a firewall is an autonomous system, making decision only with its internal rules.

The figure 3 shows the representation of the 2 security tools. As displayed, certificate cover a larger security perimeter than the firewall but is less reactive.

3.5 MANET counter-measures definition

Some recent papers provide interesting surveys of different countermeasures on MANETs Ngadi et al. (2008), Satria Mandala & Abdullah (2006). Some papers provide security

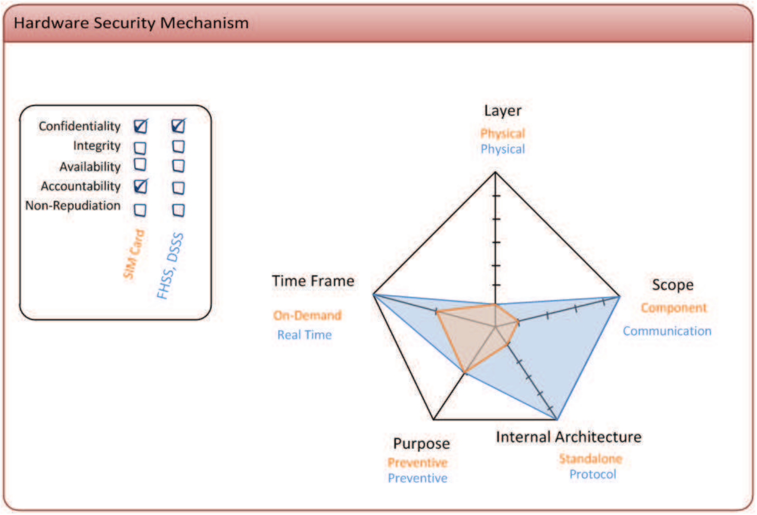


Fig. 4. Hardware Security Mechanism Attributes

mechanisms classified by OSI layer Bing Wu (2006). In this section, security tools are organized around the previously defined categories: hardware security mechanisms, protocol security mechanism, software security mechanism.

3.5.1 Hardware security mechanism

MANETs are composed of a set of mobile components. Mobile components can be smart phone, laptop, PDA, probes. Such component can hold physical protection against unauthorized use. Common mechanism like SIM cards rely on a PIN code to access to the component. More sophisticated approaches use biometrics mechanisms (fingerprint, Iris identification), token or smart card for components authentication. The security attributes definition of SIM cards are displayed in blue in the figure 4.
Moreover, wireless MANET communications can be intercepted by anyone monitoring Radio Frequency spectrum. As explained before, MANET communications can be jammed or interfered, creating loses of data integrity or denial of service. FHSS Stallings (2002) modulates the signal with radio frequency series avoiding signal discovering or jamming. DSSS Stallings (2002) is another solution by modulating each bit of the communication with a "spreading code". The spreading code spreads the signal across a wider frequency band in proportion to the number of bit used. Such technique shares similar security attributes but covers different security goals (displayed in orange in the figure 4).

3.5.2 Protocol security mechanism

Communication protocol recommendation:
The 802.11 IEEE (2007) norm provides recommendation to secure communication in wireless environments. Encryption protocols such as WEP, WPA are specified to ensure confidentiality between wireless communications.
Routing security protocol:
As defined in section 1, collaboration between mobile components is used to route information across the network. This collaboration can lead to attacks such as Black Hole, Worm hole,

Routing table overflow, Sleep deprivation or location disclosure. Main efforts have been made to secure MANET routing protocol. Khan (2004) provide a survey of major types of secure routing protocol. Secure Routing Protocol (SRP) Papadimitratos et al. (2006) secures the MANET systems against the network topology discovering. SRP is a secure variant of the Dynamic Source Routing (DSR) Johnson & Broch (2001). It uses symmetric-key authentication (MACs) between the source and the target nodes. There is only end-to-end authentication. The route is sent to the trust destinations and the replies travel through the same route. This routing protocol avoids black whole attack.

Packet Leashes Hu et al. (2003a) is keeping constraints on packet in a Temporal or Geographical way. In the case of the Geographical constraints, the following information can be computed and kept:

– Where in location information and loosely synchronized clocks is used to create a leash,

– The distance between the sender and receiver is calculated nodes velocity and timestamps.

Packet Leashes avoids wormhole and can be used in addition to other routing protocol.

Secure Efficient Ad hoc Distance Vector Routing Protocol SEAD Hu et al. (2002) is a distance vector routing protocol extending the Destination Sequences Distance Vector routing protocol (DSDV) in which was added One way Hash Chain mechanism. In DSDV each node maintains routing information for all known destinations. Instead of asymmetric cryptographic operations, SEAD uses efficient one-way hash function to prevent sequence number and hop count from being modified by malicious nodes. SEAD uses the one-way hash function to authenticate the metric and the sequence number of a routing table. The receiver of the routing information authenticates also the sender. SEAD is robust against multiple uncoordinated attackers creating incorrect routing states but failed against the wormhole attack.

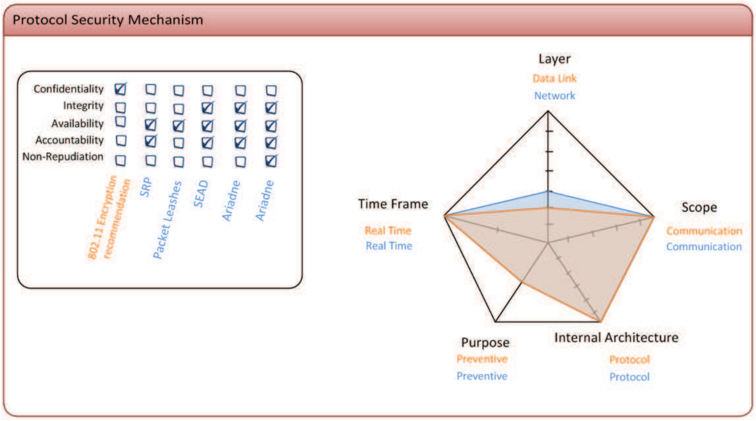
Ariadne is an on demand routing protocol Hu et al. (2005). This on demand routing protocol assumes the fact that a sending node attempts to discover a route to a destination only when it has a need to send data to that destination. In the Ariadne protocol routing messages are authenticated with 3 available schema shared secrets between each pair of nodes, Time-delayed broadcast authentication TESLA Perrig et al. (2002) and digital signatures. The route management, for its part, is done by the DSR protocol.

If the shared secret is used; each node forwarding a request includes a MAC computed with the key it shares with the target. Then, this MAC is included in a MAC list, analogous to the node list in a normal request packet. Finally, the destination checks the authentication for each hop and sent the route to the source.

If the TESLA authentication is used; each node forwarding a request includes a MAC computed using a TESLA key. The target checks TESLA security condition for each hop, then authenticates the reply message to avoid modification. Each intermediate node buffers packet until it can disclose its TESLA key, then includes key in the reply. At the end the source verifies each nodes key and MAC.

The digital signature can be used with the help of a PKI infrastructure. Each mobile component holds a certificate, each route message can be sign with the private key of the message owner. This type of authentication requires the use of effective PKI on MANET (virtual Certificate Authority Zhou & Haas (1999), certificate chaining Hubaux et al. (2001) and hybrid method Yi & Kravets (2004)). Ariadne avoids wormhole attacks.

The Authentication Routing for Ad hoc Networks (ARAN) Mahmoud et al. (2005) is an on-demand routing protocol using public key cryptography to avoid any routes modification. The ARAN protocol is used mainly on open infrastructure where network nodes can interact



Protocol Security Mechanism

	802.11 Encryption recommendation	SRP	Packet Leashes	SEAD	Ariadne	Ariadne
Confidentiality	☑	□	□	□	□	□
Integrity	□	□	□	☑	☑	☑
Availability	□	☑	☑	☑	☑	☑
Accountability	□	☑	□	☑	☑	☑
Non-Repudiation	□	□	□	□	□	☑

Fig. 5. Protocol Security Mechanism Attributes

with a fixed PKI infrastructure. ARAN protocol guaranties message authentication, integrity and non repudiation.

3.5.3 Software security mechanism

According to Satria Mandala & Abdullah (2006) MANET networks are more vulnerable than conventional networks due to their cooperative algorithms, lacks of centralized monitoring, management point and lack of clear line of defense. Intrusion Detection can be viewed as a second line of defense in MANET networks ensuring a complementary defense to preventive technique like secure routing and encryption mechanism. Intrusion Detection Systems are mainly classified into Host Intrusion detection System (HIDS) and Network Intrusion Detection System (NIDS). HIDS are in charge of the security of a single component. Verifying authorized and usage system activity (login Activity Monitoring, System Call activity Eskin et al. (2001) or incoming Network activity), HIDS detection intrusion through intrusion signature base or anomaly detection. NIDS monitors network flow (network sessions, packets content and structure Sourcefire (1998). They also sometimes compute network trends Paul Barford & Ron (2002)) located at strategic network points such as network entries (frontend or backend firewall locations) and network concentrators (switches). NIDS also use signature based and anomaly detection techniques. As MANETs are completely decentralized and do not have a fixed network infrastructure, NIDS, as known is wired network, cannot be considered in such network. HIDS are in charge of securing the local component network activity with the collaboration of other members. In this section we follow the baseline of Ngadi et al. (2008) to present some Intrusion Detection System References in MANET. The authors provide a summary of such techniques in a table comparing these research achievements on MANET IDS (figure 6).

In the Intrusion detection (ID) and Response System Zhang et al. (2003) each node holds an IDS in charge of the local component monitoring. In this approach, the monitoring is focused on user and system activities and communication activities. If an anomaly is detected, the IDS system launches a local response. If the IDS is not able to launch itself a response, collaboration with neighbors is requested to launch a global reaction. Moreover, if the local system comes in an indecisiveness state, the other nodes' help is requested to make the decision.

The Local Intrusion Detection System (LIDS) Albers et al. (2002) uses mobile agents for intrusion detection. Based on a distributed and collaborative architecture, two types of messages are exchanged between LIDS nodes: intrusion alerts resulting of a local detection and data logs coming from the local monitoring information. When local LIDS detect an anomaly, if evidences are insufficient, local LIDS can ask neighbors for additional information. In case of an intrusion detection (both anomaly and misuse detection are supported), the local LIDS launches a response and informs the other nodes in the network. As soon as the intrusion alert is received by another node, this one launches an adequate response to prevent itself from the detected attack.

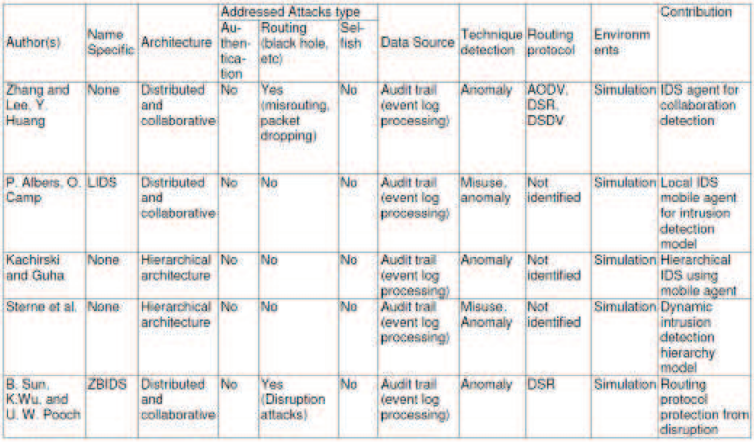
Kachirski & Guha (2003) describes a Multisensor Intrusion Detection System where each nodes hold the following function.

- Monitoring function is in charge of detecting User-Level, System Level and Packet level intrusion,
- Decision function aims at identifying anomalies as intrusion and selecting countermeasure actions,
- Action function ensures the local execution of the countermeasure actions.

In such IDS method, some nodes are selected to monitor networks activity and make global decisions. Such nodes receive alert reports from all nodes in charged. Each node is associated to a threat level defining if the node is compromised or not. When a threat level is exceeded in the global decision, an order is sent to all nodes to launch a specific action against the compromised node.

A Dynamic intrusion detection hierarchy Sterne et al. (2005) provides an approach similar to Kachirski & Guha (2003). Nodes in the network are distinguished in ”cluster head” nodes in charge of ”cluster leaf” nodes. Each node aims at monitoring, logging, analyzing, responding and reporting to cluster heads. Head cluster nodes are in charge of additional tasks such as gathering received data (fusion), filtering data, high level intrusion detection. The main point of the Sterne et al. (2005) is its capability of cascading different cluster head nodes levels. This property allows the IDS architecture to be scalable.

Zone Based IDS (ZIDS) Sun et al. (2003) try to solve the alert aggregation issue. Assuming the fact that, in collaborative environments, security mechanisms can be flooded by security alert,



Author(s)	Name Specific	Architecture	Addressed Attacks type			Data Source	Technique detection	Routing protocol	Environments	Contribution
			Authentication	Routing (black hole, etc)	Selfish					
Zhang and Lee, Y. Huang	None	Distributed and collaborative	No	Yes (misrouting, packet dropping)	No	Audit trail (event log processing)	Anomaly	AODV, DSR, DSDV	Simulation	IDS agent for collaboration detection
P. Albers, O. Camp	LIDS	Distributed and collaborative	No	No	No	Audit trail (event log processing)	Misuse, anomaly	Not identified	Simulation	Local IDS mobile agent for intrusion detection model
Kachirski and Guha	None	Hierarchical architecture	No	No	No	Audit trail (event log processing)	Anomaly	Not identified	Simulation	Hierarchical IDS using mobile agent
Sterne et al.	None	Hierarchical architecture	No	No	No	Audit trail (event log processing)	Misuse, Anomaly	Not identified	Simulation	Dynamic intrusion detection hierarchy model
B. Sun, K.Wu, and U. W. Pooch	ZBIDS	Distributed and collaborative	No	Yes (Disruption attacks)	No	Audit trail (event log processing)	Anomaly	DSR	Simulation	Routing protocol protection from disruption

Fig. 6. Comparison researches achievement on the MANET IDS Ngadi et al. (2008)

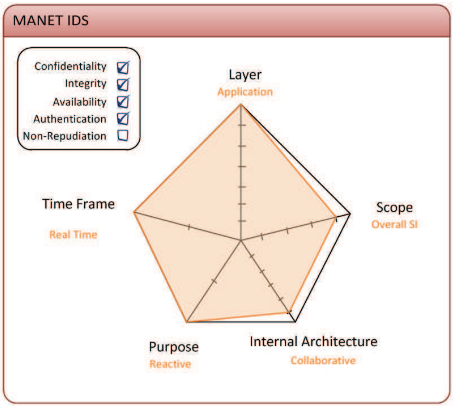


Fig. 7. Software Security Mechanism

the authors suggest the presence of alert concentration points gathering similar security alerts. The scalability issue is also targeted. By providing a non-overlapping zone-based framework, ZIDS selects a set of zones of a suitable size. When an intrusion is detected by a node, the alert message is broadcasted to all nodes of the current zone. Nodes in the same zone simply forward the received alerts. Nodes belonging to inter-zone (belonging to 2 different zones) receiving such alerts would aggregate and correlate alerts before generating alarms in the second zone.

All MANET IDS needs cooperation to prevent network and nodes from malicious activities. This collaboration is made through a collaborative architecture. MANET IDS mainly provide higher layers protection, detecting and responding when signatures or anomalies are detected on monitored users and application logs. MANET IDS share similar security attributes: preventing system against vulnerability exploit on data confidentiality and integrity, system authentication and then node availability (figure 7).

4. Conclusion / discussion

In this paper, we provide a survey of current attacks and countermeasures on MANETs. The main MANET properties imply a routing protocol collaboration and reputation mechanisms to share services. Such collaboration creates new types of attacks. Most of these attacks intent to disable the routing protocol (section 2). Threats on MANETs range from the wireless communication DoS to the service providing disturbing and fishing. Numbers of new attacks target the MANET properties such as radio communication medium, protocol collaboration and application collaboration. Mapping MANET attacks to the attack classification of Paulauskas & Garsva (2006) allows us to better clarify MANET attack properties and to easily compare MANET and non-MANET attacks. The classification allows also the attacks comparison and can help selecting the appropriate countermeasures. A survey of current security tools on MANET has been done in the second part of our document. This survey distinguishes the countermeasures available on hardware, protocol and software parts of MANETs. By providing 6 security tools properties (Protect purpose, OSI Layer, Time Frame, Purpose, Internal Architecture, Scope), these security tools can be classified and compared. Moreover, with the help of a graphical representation, the scope and purpose of security tools are highlighted allow a quick comparison.

As described in the paper, despite the emergence of new attacks, several security tools are available to protect MANETs. Nevertheless, the best security mechanisms imply, most of the time, strong requirements (deployed PKI) or consume lots of resources. Attacks on security tools themselves appear; they use the collaboration as attack vector. The reputation of collaborative nodes involved in a security mechanism becomes one of the best solutions to prevent evasion and security tool DoS. In this collaboration context, to guarantee of a security level, the main requirements are that there are more legitimate nodes than malicious nodes in the network. A virus propagation or false information divulgation can quickly disturb the entire network.

Despite great security challenges, the apparition of more and more equipments communicating together and the need of always and anywhere available services enforce the MANET growth. Nevertheless, services providing growth faster than security solutions.

5. Acknowledgment

The authors would like to thank LogLogic for its support and for allowing them to work on innovative security monitoring projects.

6. References

Albers, P., Camp, O., Percher, J.-M., Jouga, B., Mé, L. & Puttini, R. S. (2002). Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches, *Wireless Information Systems*, pp. 1–12.

Awerbuch, B., Holmer, D., Nita-Rotaru, C. & Rubens, H. (2002). An on-demand secure routing protocol resilient to byzantine failures, *WiSE '02: Proceedings of the 1st ACM workshop on Wireless security*, ACM, New York, NY, USA, pp. 21–30.

Baadache, A. & Belmehdi, A. (2010). Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks, *International Journal of Computer Science and Information Security (IJCSIS)* 7: 10–16.

Bing Wu, Jianmin Chen, J. W. M. C. (2006). A survey on attacks and countermeasures in mobile ad hoc networks, *WIRELESS / MOBILE NETWORK SECURITY* 6: Springer.

Cheswick, W. R. & Bellovin, S. M. (1994). *Firewalls and Internet SecurityRepelling the Wily Hacker*, Addison-Wesley.

COBIT (2007). *Technical report*, The IT Governance Institute (ITGI).

Cohen, F. B. (1995). *Protection and security on the information superhighway*, John Wiley & Sons, Inc., New York, NY, USA.

Cohen, F. B. (1997). Information system attacks: A preliminary classification scheme, *Computers and Security* 16, No. 1: 29–46.

Curry, D. & Debar, H. (2007). Intrusion detection message exchange format. http://www.ietf.org/rfc/rfc4765.txt.

Debar, H., Dacier, M. & Wespi, A. (1999). Towards a taxonomy of intrusion-detection systems, *Comput. Netw.* 31: 805–822.

Eckmann, S. T., Vigna, G. & Kemmerer, R. A. (2002). STATL: an attack language for state-based intrusion detection, *J. Comput. Secur* 10: 71–103.

Eskin, E., Lee, W. & Stolfo, S. J. (2001). Modelling system calls for intrusion detection with dynamic window sizes, *the DARPA Conference and Exposition on Information Survivability. DISCEX '01*.

Howard, J. D. (April 1997). *An Analysis of Security Incidents on the Internet -normalement phd* *dissertation-*, PhD thesis, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213 USA.

Howard, J. & Longstaff, T. (1998). A common language for computer security incidents, *Sand98-8667*, Sandia International Laboratories.

Hu, Y.-C., Johnson, D. B. & Perrig, A. (2002). Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks, *Mobile Computing Systems and Applications, IEEE Workshop on* 0: 3.

Hu, Y. C., Perrig, A. & Johnson, D. B. (2003a). Packet leashes: a defense against wormhole attacks in wireless networks, *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE*, Vol. 3, pp. 1976–1986.

Hu, Y.-C., Perrig, A. & Johnson, D. B. (2003b). Rushing attacks and defense in wireless ad hoc network routing protocols, *WiSe '03: Proceedings of the 2nd ACM workshop on Wireless security*, ACM, New York, NY, USA, pp. 30–40.

Hu, Y.-C., Perrig, A. & Johnson, D. B. (2005). Ariadne: a secure on-demand routing protocol for ad hoc networks, *Wirel. Netw.* 11: 21–38.

Hubaux, J.-P., Buttyán, L. & Capkun, S. (2001). The quest for security in mobile ad hoc networks, *MobiHoc '01: Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, ACM, New York, NY, USA, pp. 146–155.

IEEE (2007). Ieee 802.11: Lan/man wireless lans.

Ilyas, M. & Dorf, R. C. (2003). *The handbook of ad hoc wireless networks*, CRC Press, Inc., Boca Raton, FL, USA.

ISO-IEC (1994). Open systems interconnection (osi) – basic reference model.

ISO 27000 series (2005). *Technical report*, International Organization for Standardization.

Johnson, David B., M. D. A. & Broch, J. (2001). Dsr: the dynamic source routing protocol for multihop wireless ad hoc networks, *Ad hoc networking* 1: 139–172.

Kachirski, O. & Guha, R. (2003). Effective intrusion detection using multiple sensors in wireless ad hoc networks, *HICSS '03: Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03) - Track 2*, IEEE Computer Society, Washington, DC, USA, p. 57.1.

Khan, O. A. (2004). A survey of secure routing techniques for manet, National University of Computer and Emerging Sciences, Karachi Campus.

Lindqvist, U. & Jonsson, E. (1997). How to systematically classify computer security intrusions, *In proceeding of the IEEE Symposium on Security and Privacy* 1: 154–163.

Mahmoud, A., Sameh, A. & El Kassas, S. (2005). Authenticated routing for ad hoc networks protocol and misbehaving nodes, *TELE-INFO'05: Proceedings of the 4th WSEAS International Conference on Telecommunications and Informatics*, World Scientific and Engineering Academy and Society (WSEAS), Stevens Point, Wisconsin, USA, pp. 1–5.

Martin Rehak, Michal Pechoucek, P. C. J. N. P. M. (2008). Camnep: Agent-based network intrusion detection system (short paper), *AAMAS'08 (Autonomous Agents and MultiAgent Systems).*

Neumann, P. G. (1994). *Computer-Related Risks*, Addison-Wesley.

Neumann, P. G. & Parker, D. B. (1989). A summary of computer misuse techniques, *Proceedings of the 12th National Computer Security Conference*, Baltimore, Maryland, pp. 396–407.

Ngadi, M. A., Abdullah, A. H. & Mandala, S. (2008). A survey on manet intrusion detection, *International Journal of Computer Science and Security* 2: 1–11.

Padmavathi, G. & Shanmugapriya, D. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks, *IJCSIS International journal of Computer Science* *and Information Security* 4: 117–125.

Papadimitratos, P., Haas, Z. J. & Hubaux, J.-P. (2006). How to specify and how to prove correctness of secure routing protocols for manet, *BROADNETS*.

Paul Barford, Jeffery Kline, D. P. & Ron, A. (2002). A signal analysis of network traffic anomalies, *IMW '02: Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*, ACM Press, New York, NY, USA, pp. 71–82.

Paulauskas, N. & Garsva, E. (2006). Computer system attack classification, *Electronics and Electrical Engineering* 2: 84–87.

Perrig, A., Canetti, R., Tygar, J. D. & Song, D. (2002). The tesla broadcast authentication protocol, *RSA CryptoBytes* 5: 2002.

S. Staniford-Chen, S. Cheung, R. C. M. D. J. F. J. H. K. L. C. W. R. Y. & Zerkle, D. (1996). Grids – a graph-based intrusion detection system for large networks, *Proceedings of the 19th National Information Systems Security Conference*.

Satria Mandala, M. A. N. & Abdullah, A. H. (2006). A survey on manet intrusion detection, *International Journal of Computer Science and Security (IJCSS)* 2: 1.

Sourcefire (1998). Snort open source network intrusion prevention and detection system, http://www.snort.org/.

Stallings, W. (1995). *Network and internetwork security: principles and practice*, Prentice-Hall, Inc, Upper Saddle River, NJ, USA.

Stallings, W. (2002). Wireless communication and networks,, Pearson Education.

Staniford-Chen, .S, T. B. & Schnackenberg, D. (1998). The common intrusion detection framework (CIDF), *The Information Survivability Workshop (ISW '98)*, CERT Coordination Center, Software Engineering Institute, Orlando, FL.

Sterne, D., Balasubramanyam, P., Carman, D., Wilson, B., Talpade, R., Ko, C., Balupari, R., Tseng, C.-Y., Bowen, T., Levitt, K. & Rowe, J. (2005). A general cooperative intrusion detection architecture for manets, *IWIA '05: Proceedings of the Third IEEE International Workshop on Information Assurance*, IEEE Computer Society, Washington, DC, USA, pp. 57–70.

Sun, B., Wu, K. & Pooch, U. W. (2003). Alert aggregation in mobile ad hoc networks, *WiSe '03: Proceedings of the 2nd ACM workshop on Wireless security*, ACM, New York, NY, USA, pp. 69–78.

T. Duval, B. J. & Roger, L. (2004). Xmeta a bayesian approach for computer forensics, *ACSAC 2004 WIP Session*.

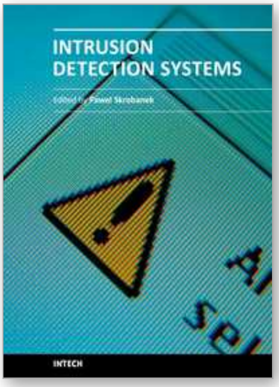
Undercoffer, J. L., Joshi, A. & Pinkston, J. (2003). Modeling computer attacks an ontology for intrusion detections, *in* LNCS-2516 (ed.), *The Sixth International Symposium on Recent Advances in Intrusion Detection*, Springer.

Yi, S. & Kravets, R. H. (2004). Composite key management for ad hoc networks, *Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004. The First Annual International Conference on*, pp. 52–61.

Zhang, Y., Lee, W. & Huang, Y.-A. (2003). Intrusion detection techniques for mobile wireless networks, *Wirel. Netw.* 9(5): 545–556.

Zheng Zhang, Jun Li, C. M. J. J. & Ucles, J. (2001). Hide: A hierarchical network intrusion detection system using statistical preprocessing and neural network classification, *the 2001 IEEE Workshop on Information Assurance and Security*.

Zhou, L. & Haas, Z. J. (1999). Securing ad hoc networks, *IEEE Network Magazine* 13: 24–30.



Intrusion Detection Systems
Edited by Dr. Pawel Skrobanek

ISBN 978-953-307-167-1
Hard cover, 324 pages
Publisher InTech
Published online 22, March, 2011
Published in print edition March, 2011

The current structure of the chapters reflects the key aspects discussed in the papers but the papers themselves contain more additional interesting information: examples of a practical application and results obtained for existing networks as well as results of experiments confirming efficacy of a synergistic analysis of anomaly detection and signature detection, and application of interesting solutions, such as an analysis of the anomalies of user behaviors and many others.

How to reference
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Jacques Saraydayran, Fatiha Benali and Luc Paffumi (2011). A Survey on new Threats and Countermeasures on Emerging Networks, Intrusion Detection Systems, Dr. Pawel Skrobanek (Ed.), ISBN: 978-953-307-167-1, InTech, Available from: http://www.intechopen.com/books/intrusion-detection-systems/a-survey-on-new-threats-and-countermeasures-on-emerging-networks

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821