International Journal of Engineering Innovation & Research
Volume 4, Issue 5, ISSN: 2277 – 5668

Information Security Management in Mobile Ad Hoc Networks

ECHCHAACHOUI Adel*, ELKOUTBI Mohammed
SIME Laboratory, E.N.S.I.A.S, Mohammed 5 University, Rabat, Morocco
*Email: adel.echchaachoui@um5s.net.ma

***Abstract* – Several and different research work was carried out to secure the data routing in MANETs. The proposed solutions differ depending on the problematic treated and the approach used. Although the goal is unique, but the lack of a methodical system in terms of study, upgrade and continuous improvement, makes these works ineffectivewithin a global framework of security. In this article, we use systematic methods of information security management and risk management in MANETs, through a series of process of ISO/IEC 27000 standard. Our study showed that it is essential to establish corrective and improvement actions for a best management of resources and incidents, and implement sequentially security measures for better risk management in mobile Ad hoc networks.**

***Keywords* – MANET, Security, Risk, Management, Standard.**

I. Introduction

Mobile Ad Hoc Network (MANET) provide an ideal environment for the users and a rich field for the researchers and specialist engineers. Indeed, their deployments do not require the establishment of an infrastructure or the installation of a control and management center, providing a flexible exchange of information in a fully mobile environment. These basic criteria of MANETs, are very affluent areas and subjects for the search and the technology development, to improve communication systems in security, quality of service, availability, performance, and management.In terms of security, several research works was carried out, through which the authors proposed different solutions and approaches to secure communications in MANETs[1], such as the detection of a specials attack or intrusion. These works had as main objective to solve, each time, a particular security problem without defining a general security policy and follow a clear and structured approach to better improve and manage security of the information system.In this article, we study the data security system of the OLSR, by building on the international standard ISO 27000, to provide best practices and recommendations on the selection and the implementation of security measures, and implement an information security system, which will based on a methodical approach of risk management.This article consists of five sections. In Section 2, we cite and analyze the similar works. Section 3 is consecrated to the presentation of the ISO/CEI 27000 standard.In Section 4, we apply the ISO 27002 standard in the OLSR routing system to highlight the aspects and the basic criteria that must be considered, before improve information security in MANETs. In Section 5, we study and analyze the security risks concerning OLSR, according to the requirements of the ISO 27005 standard.

II. Related Work

In [2], the authors presented a security analysis model of the information system in the field of cloud computing, with reference to ISO 27005. The proposed model treated the identification of assets and the establishment of context. The authors did not address an important axis required by the standard, which are the identification of vulnerabilities and threats and risk measurement.
The authors of [3] presented a study of attack and defense based on a risk management model.

For the authors of this article, the concept of risk is a function that depends on the likelihood of the threat and its impact on the system.The authors did not introduce the valuation of assets in their formulation. Yet, it is a major criterion to be taken into account in risk analysis.

In [4] the authors present the routing protocols and security models proposed in previous years to secure data routing in MANETs.

The authors have studied the approaches proposed previously and have concluded that the solutions proposed by the researchers cannot adequately solve the problem of security for one simple reason: lack of a common definition of security. For the authors, to achieve this goal, we need to know the environment in which a routing protocol will be secure, and vulnerabilities will not be exploited.

The authors of [5] presented the vulnerabilities, attack types and the main proposed solutions of security in MANETS.

The authors proposed a new concept of survivability in MANETs to secure routing traffic regardless of the level or the type of attack. The concept addresses three aspects:

- The route discovery
- The data transmission
- The key management and access control

The authors claim that the implementation of better security approach requires the use of corrective and preventive actions.

In [6], the authors analyzed the security of route discovery protocols in MANETs, in a general context.

They proposed a new approach called "composability" viewed as an essential component in the security of routing in MANETs.

The authors of [7] presented the best known types of attacks in MANETs and proposed solutions for the detection of each of these attacks.

These restricted models cannot provide effective security system since they target specific problems.

The authors of [8] studied the routing protocols in ad hoc networks in terms of routing and security. They classified OLSR among the protocols that do not include a security system.

III. ISO/CEI 27000

ISO / IEC 27000 is a series of information security standards.

It comprises over 40 standards. The best known and most used areprincipally (as shown in Fig.1):

ISO/IEC 27001: Information security management systems - Requirements

ISO/IEC 27002: information security management - Code of practice

ISO/IEC 27003: Information security management - system implementation guidance

ISO/IEC 27004: Information security management - Measurement

ISO/IEC 27005: Information security risk management.

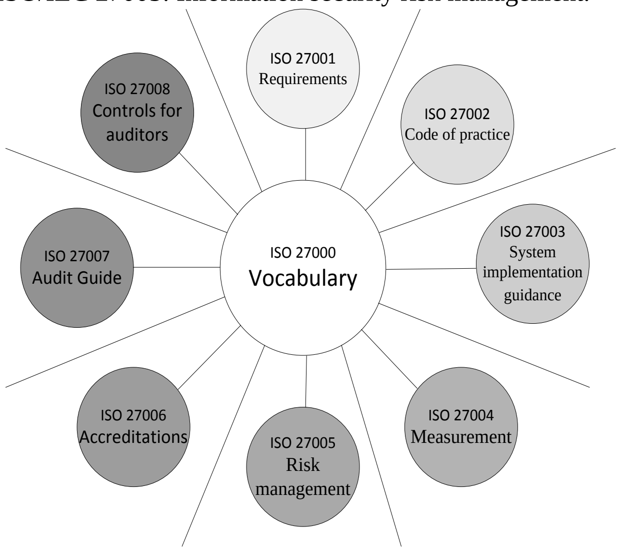


Fig. 1 ISO/IEC 27000 Series

Figure Source: Self drawing

The ISO 27000 standard is often applied in organizations and companies wishing to implement a management system for information security. In our case, we talk about a protocol of data transmission. The standard does not define the context and environment of its implementation. In addition, standards-based systems engineering work has already been completed [9]. Despite that, we consulted an expert, which is Anne Lupfer author of a book on risk management of securiy information, and we asked her about responsibility and scope of the standard. Ms. Lupfer said that it is quite possible to create a systematic approach based on the ISO 27000 standard for a computer communication protocol, provided to define the corresponding perimeter. Ms. Lupferus clarify that it is more profitable to build our study on the knowledge and skills of our team in the application of the standard, while appealing to an expert to confirm best practices.

IV. Application of ISO 27002 on OLSR

A. ISO 27002

The International Organization for Standardization defines the ISO 27000 standard as follows:

« ISO/IEC 27002 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s). »

ISO 27002 is a set of good practices presented in the form of measures, which are divided (As shown in Table 1) into 11 fields (or chapters), 39 objectives and 133 controls.

Table 1: ISO 27002 fields

Field	Designation
1	Chapter 5 : Security Policy
2	Chapter 6 : Organization of information security
3	Chapter 7 : Asset management
4	Chapter 8 : Human resources security
5	Chapter 9 : Physical and environmental security
6	Chapter 10 : Communications and operations management
7	Chapter 11 : Access control
8	Chapter 12 : Information systems acquisition, development and maintenance
9	Chapter 13 : Information security incident management
10	Chapter 14 : Business continuity management
11	Chapter 15 : Compliance

Table Source: Self drawing

B. Application of ISO 27002

(a) Scope of study

The scope of our case study concerns the OLSR routing protocol in Ad hoc networks. This is a system for processing and exchanging data between the computer equipment (nodes) that use radio transmissions for sending and receiving information.The measures we have applied in our case are shown in Table 2.

Table 2: ISO 27002 fields concerning olsr

Case	Field	Objective	Control
OLSR	Chapter 5 : Security Policy	5.1	5.1.1, 5.1.2
	Chapter 6 : Organization of information security	6.1, 6.2	6.1.1, 6.1.3, 6.2.1, 6.2.2
	Chapter 7 : Asset management	7.1, 7.2	7.1.1, 7.1.2, 7.1.3, 7.2.1, 7.2.2
	Chapter 10 : Communications and operations management	10.1, 10.8, 10.10	10.4.1, 10.8.1, 10.10.3
	Chapter 11 : Access control	11.1, 11.4, 11.5	11.1.1, 11.4.7, 11.5.2
	Chapter 12 : Information systems acquisition, development and maintenance	12.2, 12.3	12.2.3, 12.3.1, 12.3.2
	Chapter 13 : Information security incident management	13.1, 13.2	13.1.1, 13.1.2, 13.2.2
	Chapter 14 : Business continuity management	14.1	14.1.2
	Chapter 15 : Compliance	15.1	15.1.3

Table Source: Self drawi

(b) Application measures

The application of the ISO 27002 standard for OLSR concerned 9 fields, 17 control and 25 objectives.

Our study and application of the standard on the OLSR, has resulted in a state of security of this protocol, which we present in Table 3.

Table 3: State of security of olsr

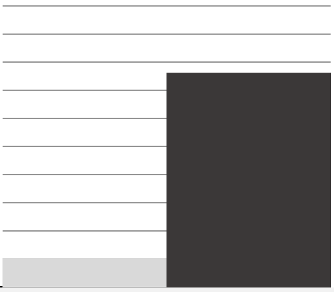
Objectives ISO 27002	Fields ISO 27002	Odds	%	Targeted Notes	%	Odds ISO 27002	Targeted Notes ISO 27002
1	Ch.5 Security Policy	0,0	0,00%	3,0	60,00%		
2	Ch.6 : Organization of information security	0,0	0,00%	2,3	45,00%		
2	Ch.7 : Asset management	1,2	24,00%	3,0	60,00%		
3	Ch.10 : Communications and operations management	0,8	15,00%	2,8	55,00%		
3	Ch.11 : Access control	2,7	53,33%	5,0	100,00%		
2	Ch.12 : Information systems acquisition, development and maintenance	0,0	0,00%	4,7	93,33%		
2	Ch.13 : Information security incident management	0,0	0,00%	4,7	93,33%		
1	Ch.14 : Business continuity management	0,0	0,00%	4,0	80,00%		
1	Ch.15 : Compliance	0,0	0,00%	5,0	100,00%		
17	**9**					**10,26%**	**76,30%**

Table Source : Self drawing

These results showed that the current state of the OLSR only meets 10,26% of security requirements specified by the standard ISO 27002, against a minimal target of 76,30%.

The gap between these two security levels is enormous.

In Fig.2, we present the portrait of the current state and the target state of security concerning OLSR.

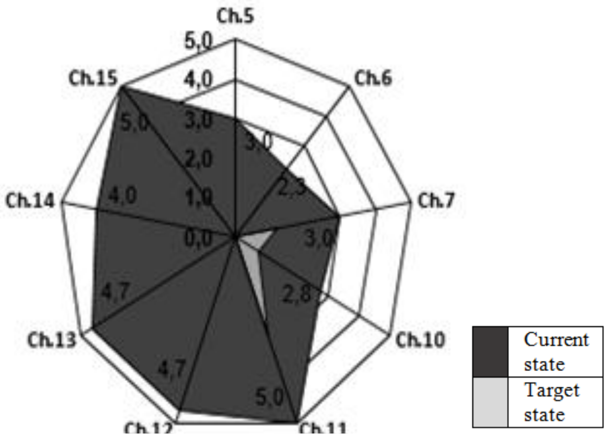


Fig. 2 Portrait of the OLSR about his State of security

Figure Source: Self drawing

We can deduce from this portrait, that it is essential to carry out corrective actions in six axis: Ch.5, Ch.6, Ch.12, Ch.13, Ch.14 and Ch.15.Achieving the upgrade actions is also essential and concerns three axis: Ch.7, Ch.10 and Ch.11.

Several actions were proposed through research to improve the security of OLSR. To know the actions of correction and upgrades that must be achieved, we have established the Table 4 concerning the status of controls and actions.

Table 4: State of controls and actions of OLSR

Field	Control	Action performed	Action not performed
Ch.5 Security Policy	5.1.1: Information security policy document	■ [10-12]	
	5.1.2: Review of the information security policy		
Ch.6 : Organization of information security	6.1.1: Management commitment to information security		
	6.1.3: Allocation of information security responsibilities		
	6.2.1: Identification of risks related to external parties	■ [13]	
	6.2.2: Addressing security when dealing with customers		
Ch.7 : Asset management	7.1.1: Inventory of assets		■
	7.1.2: Ownership of assets		■
	7.1.3: Acceptable use of assets		■
	7.2.1: Classification guidelines		■
	7.2.2 : Information labeling and handling		■
Ch.10 : Communications and operations management	10.4.1 : Controls against malicious code	■ [14, 15]	
	10.5.1 : Information back-up	■ [16]	
	10.8.1 : Information exchange policies and procedures	■ [17]	
Ch.11 : Access control	11.1.1 : Access control policy	■ [18]	
	11.4.7 : Network routing control	■ [19]	
	11.5.2 : User identification and authentication		
Ch.12 : Information systems acquisition, development and maintenance	12.2.3 : Message integrity		
	12.3.1 : Policy on the use of cryptographic controls		
	12.3.2 :Key management.		
Ch.13 : Information security incident management	13.1.1 : Reporting information security events		
	13.1.2 : Reporting security weaknesses		■
	13.2.2 : Learning from information security incidents		■
Ch.14 : Business continuity management	14.1.2 : Business continuity and risk assessment		■
Ch.15 : Compliance	15.1.3 : Protection of organizational records	■ [20]	

Table Source: Self drawing

The actions to be takenare divided into two categories:
1. Corrective actions relate the fields 13 and 14 (incident management and business continuity plan).
2. Actions of upgrade relate the field 7 (Asset Management).

In Table 5, we list the actions and the corresponding controls that should be carried.

Table 4: Actions categories

Field / Control		Action	Type of action	Note
Field	Ch.7 : Asset management	Define the level of relevance in the management of the OLSR by the implementation of an information classification plan.	Upgrade	These actions are processed by ISO 27005
Control	13.1.2 : Reporting security weaknesses	Study and Perform risk management of the OLSR	Correction	
	13.2.2 : Learning from information security incidents			
	14.1.2 : Business continuity and risk assessment			

Table Source: Self drawing

V. Application of ISO 27005 on OLSR

A. ISO 27005

The International Organization for Standardization defines the ISO 27005 standard as follows:

« ISO/IEC 27005 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach ».

The ISO 27005 standard follows a pattern of continuous improvement that is based on four steps (As in Fig. 3):

1. Plan: Plan what needs to be achieved in relation to objectives
2. Do: Carry out the planned actions
3. Check: Ensure the proper implementation of the actions
4. Act: Define the corrective and preventive actions.

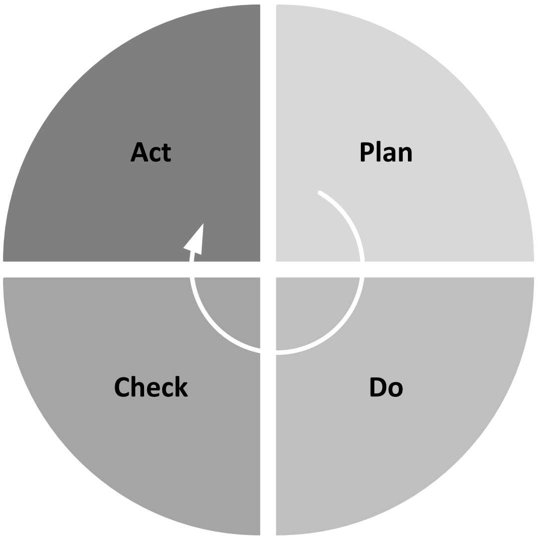


Fig. 3 PDCA cycle

Figure Source: Self drawing

ISO 27005 is aninformation security management process that includes the definition of objectives, constraints and risks, their assessment and applications according to a risk treatment plan to implement the recommendations and decisions.

This approach is used to analyze and predict incidents and their consequences and impacts on the system.

The process of ISO 27005 consists of the following phases:

1. Establishment of context
2. Risk assessment
2.1. Risk Analysis
2.1.1. Risk identification
2.1.2. Risk Estimation
2.2. Risk assessment
3. Risk treatment
4. Acceptance of risk

B. Application of ISO 27005

(a) Establishment of context

Context

• Computer entities (nodes) use OLSR as the routing protocol for sending and receiving data in a mobile wireless network (called mobile Ad Hoc or MANET)

• Each node stores information about architecture and network topology in its internal memory.

• Nodes use batteries as their only source of energy.

• Nodes exchange the information between them constantly.

• For sending the routing information, the nodes use the free space for establish radio transmissions.

• Data are broadcasted in clear.

Assets

In our context, assets are divided into two types: Primary asset and Supporting asset, as shown in Table 6.

Table 5: Assets of olsr

Assets List			
Asset			Property
Primary Asset	1	HELLO Message	OLSR
	2	TC Message	OLSR
	3	DATA	OLSR
	5	MPR	OLSR
Supporting Asset	6	Radio	USER
	7	Battery	USER
	8	Node	USER

Table source: Self drawing

(b) Vulnerabilities and Threats

Vulnerabilities

The most significant vulnerabilities of the OLSR are [21]:

1. Data in the air: the data are transmitted in the air and can be intercepted by all nodes.
2. Dynamic topology: nodes frequently change their positions. Therefore, routing data are continually changing, making difficult to control errors.
3. No control: the lack of a control center does not allow management the exchange and centralized processing of critical information.
4. Open access: in the absence of an authentication system, the nodes cannot identify malicious nodes during the initiation of exchange.
5. Radio :the only medium of communication in MANETs are radio transmissions. If the radio space is disturbed, network performance can drop considerably.
6. Battery: the only energy source nodes is the battery. In case of exhaustion, the node will be down.

Threats

In their article, [22], the authors defined the main types of threats in Ad hoc networks, dividing them into two categories: internal threats and external threats.

Example of external threats:

- The Listening traffic: the interception and reading of data circulating in the network
- The Active Interference: sending signals to cause radio interference and reduce network performance

Internal threats, which are more dangerous, are mainly:

- The failed nodes
- Bad failed nodes
- Selfish nodes

- Malicious nodes

(c) Criteria

Chapter 7.2 of the ISO 27005 standard defines three types of criteria:

Impact criteria, risk evaluation criteria and risk acceptance criteria.

- **Impact criteria**

The impact criteria are thresholds that must be defined in this section. They provide a basis from which the risk will be taken into account in the risk analysis.

Besides the three criteria mentioned by the standard (Confidentiality, Integrity, Availability) we added the criterion of authentication to our case study, given its importance in information security in MANETs.

Table 7 lists the different levels and criteria of impacts we have identified.

Table 6: Impact criteria

Level	**Confidentiality** (C)	**Integrity** (I)	**Availability** (D)	**Authentication** (A)
1	Public	Discoverable	Over 5s	No authentication
2	Limited	Mastered	Between 2s and 5s	Simple Authentication
3	Reserved	Integrates	Between 1s et 2s	Strong Authentication
4	Private		Less than 1s	

Table source: Self drawing

- **Risk Assessment Criteria**

This is the definition of the risk levels for which the risk needs to be treated.ISO 27005 specifies in Annex E, a measuring table of the level of risk from the valuation of assets, levels of vulnerabilities and threats, as mentioned in Table 8.

Table 7: Risk Assessment criteria

	Likelihood of Threat operating	**Low**			**Medium**			**High**		
	Ease of operation	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Table source: Self drawing

Based on this information, we have established a table about risk assessment of the OLSR, which we present in Table 9.

Table 8: Risk Assessment

Asset	**Valuation**				**Vulnerabilities**		**Threats**		**Risk level**
	C	**I**	**D**	**A**	**Type**	**Level**	**Type**	**Level**	
HELLO Message	0	2	1	1	V_1 : Data in the air	M	External Passive attack	M	4
					V_2 : Dynamic topology	L	Internal Active attack	H	4
					V_3 : No control	L			4
					V_4 : Open access	M			5
TC Message	0	2	2	1	V_1 : Data in the air	M	External Passive attack	M	5
					V_2 : Dynamic topology	L	Internal Active attack	H	5
					V_3 : No control	L			5
					V_4 : Open access	M			6
DATA	3	3	4	3	V_1 : Data in the air	H	External Passive attack	M	7
					V_2 : Dynamic topology	M	Internal Active attack	H	7
					V_3 : No control	M			7
					V_4 : Open access	H			8
MPR	0	1	3	3	V_5 : Radio	M	External Passive attack	L	4
					V_6 : Battery	H	Internal Active attack	M	6
Node	0	1	2	3	V_5 : Radio	M	External Passive attack	L	4
					V_6 : Battery	H	Internal Active attack	M	6

Table source: Self drawing

- **Risk acceptance criteria**

The ISO 27005 standard requires (in 4.2.1.c.2 terms and 5.1.f) the definition of acceptable levels of risk to the system, without specifying how it can be done. Several approaches and methods exist for estimating the value of risk. Most of them consider the values of assets, operating levels of vulnerabilities and impacts. In our case, we define the risk estimate as follows:

Let A be an asset, and c_A, i_A, $d_A$and a_A integer values that represent respectively the valuation of the confidentiality, integrity, availability and authentication of A.

Let V = {V_1, V_2, V_3, V_4, V_5, V_6} the OLSR vulnerabilities identified in Table IX.

$V_{iA}$is the value of the likelihood of vulnerability V_i for A, where iϵ{1, 2, 3, 4, 5, 6}.

Let I_{iA} the value of the impact of the vulnerability V_i on A. $I_{iA} \epsilon \mathbb{N}$.

So, the estimated value of the exploitation level risk of the vulnerability $V_i$by a threat on Asset A with the I_{iA} impact is calculated as follows:

$$R = Max(cA, iA, dA, aA) \times [(V_{iA} \times I_{iA}) / 2]$$

Thus, the values of risk levels will be between 0 and 32.

Risk Acceptance levels that we identified in this first evaluation are mentioned in Table 10.

Table 9: Risk acceptance level

Estimative value of risk level	Acceptation Level
between 0 et 8	Acceptable
between 9 et 16	Tolerable
between 17 et 24	Unacceptable
between 25 et 32	Intolerable

Table source: Self drawing

Thus, we can deduce the table of risk acceptance of the OLSR, which we present in Table 11.

Table 10: Risk acceptance

Asset	Valuation				Vulnerabilities	Threats	Likelihood	Consequence	Impact	Risk level	Risk Acceptance level
	C	I	D	A							
HELLO Message	0	2	1	**1**	Data in the air	External Passive attack	4	Data interception and Sniffing	Very Low 1	4	Acceptable
					Dynamic topology	Internal Active attack	3	Difficulty in identifying threats and analyze risks	Low 2	6	Acceptable
					No control			Trouble at managing	High 3	9	Tolerable
					Open access			Problem to identify and access to information	Very High 4	12	Tolerable
TC Message	0	2	2	**1**	Data in the air	External Passive attack	4	Data interception and Sniffing	Very Low 1	4	Acceptable
					Dynamic topology	Internal Active attack	3	Difficulty in identifying threats and analyze risks	Low 2	6	Acceptable
					No control			Trouble at managing	High 3	9	Tolerable
					Open access			Problem to identify and access to information	Very High 4	12	Tolerable
DATA MPR	3	3	4	**3**	Data in the air	External Passive attack	4	Data interception and Sniffing	Very High 4	32	Intolerable
					Dynamic topology	Internal Active attack	3	Difficulty in identifying threats and analyze risks	High 3	18	Unacceptable
					No control			Trouble at managing	High 3	18	Unacceptable
					Open access			Problem to identify and access to information	Very High 4	24	Unacceptable
	0	1	3	3	Radio	External Passive attack	1	Disruption of communications	High 3	5	Acceptable
					Battery	Internal Active attack	2	Shutting down the node	Very High 4	12	Tolerable

Asset	0	1	2	3	Radio	External Passive attack	1	Disruption of communications	High 3	5	Acceptable
					Battery	Internal Active attack	2	Shutting down the node	Very High 4	12	Tolerable

Table source: Self drawing

(d) Action plan

Through this evaluation study, we can deduce that it is essential to implement security measures to reduce the levels of risk intolerable and unacceptable in relation to the "Data" asset. Thereafter, the system should be reassessed to measure risk levels and reduce the level of acceptance.

In Table 12, we provide solutions that will achieve these Objectives:

Table 11: Security measures

Asset	Vulnerability	Threat	Risk Acceptance Level
Data	Data in the air	Internal Active attack	Unacceptable
	Dynamic topology	External Passive attack	Intolerable
	No control		
	Open access		

Table source: Self drawing

VI. Conclusion

The massive use of mobile Ad hoc networks implies the growth of the numbers and types of threats for the security of data in these communication environments. The security system will have to be dynamic and scalable to follow the advances and the multitudes of risks. Security solutions must be studied according methodical steps before being implemented. In this paper, we applied the best practices guide of the ISO 27002 standard on OLSR to deduce the recommendations on better management of information security in MANETs.Then we reviewed and assessed the risk levels and their acceptances by a methodical approach from the ISO 27005 standard to establish a risk management system for the OLSR.

Our study identified the need to implement an asset management and incident through the implementation of an information classification plan, in terms of values, legal requirements, sensitivity and criticality, and development of procedures for processing information in accordance with the classification plan to increase the security level according to the international requirements from 10% to 76%.

The second part of the study allowed us to infer the need to include risk reduction system in managing the security of the OLSR. This process will follow two phases:

1. Taking safety measures to reduce risks in terms of data transmission.
2. Reducing the risk relative to assets (knots, HELLO and TC packets), according to a reassessment process and continuity. This will be the objective of our future work.

Acknowledgments

Our heartfelt thanks to the security and information system experts and consultants for their time and valuable comments and suggestions, which we allowed to improve the quality of our work, namely M. ZELLOU Mohammed Adil: expert in computer security, certified CISSP by ISC2, and Mr. CHAOUCH Azzouz: consultant and expert in management information systems, IRCA auditor.

References

[1] Alani, M.M., " MANET security : a survey ", in Control System, Computing and Engineering (ICCSCE), 2014 IEEE International Conference on, 2014, 559 – 564.

[2] Beckers, K., Schmidt, H. ; Kuster, J. ; Fassbender, S., "Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing", in Availability, Reliability and Security (ARES), 2011 Sixth International Conference on, 2011, pp. 327 – 333.

[3] Teixeira, A. Sch. of Electr. Eng., Dept. of Autom. Control, KTH, Stockholm, Sweden Kin Cheong Sou ; Sandberg, H. ; Johansson, K.H., "Secure Control Systems: A Quantitative Risk Management Approach", Control Systems, IEEE, Journal of, Volume:35 , Issue: 1, 2015, pp. 24 – 45.

[4] Andel, T.R., Yasinsac, A., " Surveying security analysis techniques in manet routing protocols" , Communications Surveys & Tutorials, IEEE, Journal of, Volume:9 , Issue: 4, 2007, pp. 70 – 84.

[5] Lima, M., dos Santos, A.L. ; Pujolle, G., "A survey of survivability in mobile ad hoc networks", Communications Surveys & Tutorials, IEEE (Volume:11 , Issue: 1), 2009, pp. 66 – 77.

[6] Burmester, M. , de Medeiros, B., "On the Security of Route Discovery in MANETs ", Mobile Computing, IEEE Transactions on, Journla of, Volume:8 , Issue: 9, 2009, pp. 1180 – 1188.

[7] Rajakumar, P., Prasanna, V.T. ; Pitchaikkannu, A., "Security attacks and detection schemes in MANET", Electronics and Communication Systems (ICECS), 2014 International Conference on, 2014, pp. 13-14.

[8] Mohandas, G. , Silas, S. ; Sam, S., "Survey on routing protocols on mobile adhoc networks" , Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on, 2013, pp. 514 – 517.

[9] Evans, R. , Tsohou, A. ; Tryfonas, T. ; Morgan, T., "Engineering secure systems with ISO 26702 and 27001", System of Systems Engineering (SoSE), 2010 5th International Conference on, 2010, pp. 1-6.

[10] M. Salmanian, P. C. Mason, J. Treurniet, H. Jiangxin, P. Li, and L. Ming, "A modular security architecture for managing security associations in manets," in Mobile Adhoc and Sensor Systems (MASS), 2010 IEEE 7th International Conference on, 2010, pp. 525-530.

[11] Garci, x, L. J. a Villalba, J. Garcia Matesanz, Rupe, x, *et al.*, "Secure extension to the optimised link state routing protocol," *Information Security, IET,* vol. 5, pp. 163-169, 2011.

[12] B. Kannhavong, H. Nakayama, and A. Jamalipour, "SA-OLSR: Security Aware Optimized Link State Routing for Mobile Ad Hoc Networks," in *Communications, 2008. ICC '08. IEEE International Conference on,* 2008, pp. 1464-1468.

[13] Cai Fu , Jihang Ye ; Li Zhang ; Zhang Zhang ; Yunhe Zhang, "A principal component analysis and risk assessment framework

based on Projection Pursuit in ad hoc networks", 2010, pp. 2721 – 2725.

[14] A. Adnane, C. Bidan, and R. T. de Sousa, "Trust-Based Countermeasures for Securing OLSR Protocol," in *Computational Science and Engineering, 2009. CSE '09. International Conference on*, 2009, pp. 745-752.

[15] P. Nagrath and B. Gupta, "Wormhole attacks in wireless adhoc networks and their counter measurements: A survey," in *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*, 2011, pp. 245-250.

[16] Mohite, V. , Ragha, L., " Cooperative Security Agents for MANET", Information and Communication Technologies (WICT), 2012 World Congress on, 2012, pp. 549 – 554.

[17] Jacquet, P. , Muhlethaler, P. ; Clausen, T. ; Laouiti, A. ; Qayyum, A. ; Viennot, L., " Optimized link state routing protocol for ad hoc networks ", Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International, 2001, pp. 62 – 68.

[18] Abu Bakar, A. , Ghapar, A.A. ; Ismail, R., " Access control and privacy in MANET emergency environment", Computer and Information Sciences (ICCOINS), 2014 International Conference on, 2014, pp. 3-5.

[19] Hao Yang , HaiyunLuo ; Fan Ye ; Songwu Lu ; Lixia Zhang, " Security in mobile ad hoc networks: challenges and solutions", Wireless Communications, IEEE, Journal of, Volume:11 , Issue: 1, 2004, pp. 38-47.

[20] Shuai Zhao, Le Chang ; Tong Zhao ; Wei Yan, " LCS-MANET: A mobile storage architecture with location centric storage algorithm in manets", Computing, Networking and Communications (ICNC), 2013 International Conference on, 2013, pp. 973 – 977.

[21] Azer, M.A., El-Kassas, S.M. ; El-Soudani, M.S., "Security in Ad Hoc Networks: From Vulnerability to Risk Management ", Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09. Third International Conference on, 2009, pp. 203 – 209.

[22] SarveshTanwar, Prema K.V, Threats & Security Issues in Ad hoc network: A Survey Report, "International Journal of Soft Computing and Engineering (IJSCE) ", Journal of, Volume-2, Issue-6, 2013, pp. 138 – 143.

AUTHOR'S PROFILE

ECHCHAACHOUI Adel
PHD Student in Mobile Intelligent System ENSIAS, University Mohamed V - Souissi Rabat, Morocco
Email: adel.echchaachoui@um5s.net.ma

EL KOUTBI Mohammed
Full Professor of Computer Science Networking Department ENSIAS, University Mohamed V - Souissi Rabat, Morocco
Email: elkoutbi@ensias.ma