Performance Evaluation of Security Mechanisms in RAOLSR protocol for Wireless Mesh Networks

Yesica Imelda Saavedra Benitez
Technological Institute of Toluca
ysaavedrab@ittoluca.edu.mx

Jalel Ben-Othman
Laboratory L2TI
University of Paris Nord
jalel.ben-othman@univ-paris13.fr

Jean-Pierre Claude
Laboratory CNRS-Prism
University of Versailles
jean-pierre.claude@prism.uvsq.fr

***Abstract*—In this paper, we have proposed the IBE-RAOLSR and ECDSA-RAOLSR protocols for WMNs (Wireless Mesh Networks), which contributes to security routing protocols. We have implemented the IBE (Identity Based Encryption) and ECDSA (Elliptic Curve Digital Signature Algorithm) methods to secure messages in RAOLSR (Radio Aware Optimized Link State Routing), namely TC (Topology Control) and Hello messages. We then compare the ECDSA-based RAOLSR with IBE-based RAOLSR protocols. This study shows the great benefits of the IBE technique in securing RAOLSR protocol for WMNs. Through extensive ns-3 (Network Simulator-3) simulations, results have shown that the IBE-RAOLSR outperforms the ECDSA-RAOLSR in terms of overhead and delay. Simulation results show that the utilize of the IBE-based RAOLSR provides a greater level of security with light overhead.**

A. *key word*

Security, Routing Protocol, Wireless Mesh Networks, Radio Aware Optimized Link State Routing, IBE, Identity Based Encryption.

I. Introduction

The RAOLSR [1] protocol is a Wireless Mesh Network (WMN) Protocol, which mainly focuses on the minimization of overhead flooding in the Wireless Mesh Network. The path selection protocol is based on the Optimized Link State Routing (OLSR) [2] protocol and the Fisheye State Routing (FSR) [3] protocol and uses radio aware metric for forwarding route and multipoint relay set calculation. The OLSR in general does not guarantee the integrity of routing information at any node and relies on frequent updates to minimize any node with unsynchronized routing message. Otherwise, Radio-aware OLSR (RAOLSR) has modified the frequency of TC messages updates so that local nodes receive them more frequently than distant nodes. RAOLSR protocol is an adaptation of the OLSR protocol for WMNs which reduces overhead flooding packets.

The performance of routing protocols in the wireless network varies based on the network and the selection of accurate routing protocols according to the network, which ultimately has a significant influence on the efficiency of that wireless network [4] and [5], so we propose a scheme for securing the messages in RAOLSR routing protocol.

RAOLSR realizes the detection and maintenance of optimal routes based on a predefined metric, given that each mesh point (MP) has a mechanism to define the metric cost of a link to each of its neighbors. In order that propagate the metric-link cost information between MPs, a metric field is utilized in RAOLSR protocol.

The IEEE 802.11s standard defines two basic routing protocols as shown in figure 1:

1) Hybrid wireless mesh routing protocol (HWMP).
2) Radio Aware Optimized Link State Routing (RAOLSR).

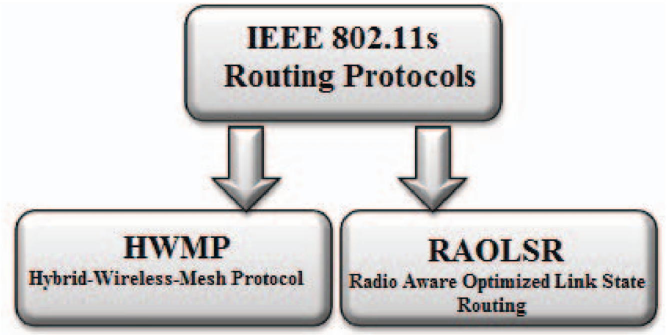
IEEE 802.11s
Routing Protocols
HWMP
Hybrid-Wireless-Mesh Protocol
RAOLSR
Radio Aware Optimized Link State Routing

Figure 1. 802.11s Protocols

The RAOLSR routing protocol for WMNs does not provide integrity and authentication in the routing HELLO and TC messages, which makes it vulnerable to many routing attacks. The contributions of this research are as follows. We propose a secure RAOLSR routing protocol using the Elliptic Curve Digital Signature and Identity Based Encryption mechanisms in order to protect the unprotected routing of information elements.

The rest of the paper has been organized as follows. In section II, we discuss related works and analyze in detail one type of attack. In Section III, we present the RAOLSR routing protocol. In Section IV, we describe ECDSA and IBE mechanisms. In Section V, We discuss the routing security issues in a we compare two schemes for securing the RAOLSR routing protocol and propose a feasible solution for RAOLSR protocol. Simulation results and their corresponding analysis for comparing the ECDSA-based RAOLSR against IBE-based RAOLSR are presented in Section VI. Conclusions of our work are provided in Section VII.

978-1-4799-2003-7/14/$31.00 ©2014 IEEE

II. Related Works

Security in proactive routing protocols based on the 802.11 standard is a continuous area of research. We list approach that are related to our work.

Several authors have proposed intrusion prevention techniques to secure the proactive routing protocols. For example, in [6], authors proposed a comparative investigation between different security mechanisms for the OLSR protocol, concluding that the best performance mechanism is ECDSA (Elliptic Curve Digital Signature Algorithm). For this reason, we compare the ECDSA-based RAOLSR against identity-based encryption (IBE)-based RAOLSR.

Ghannay et al. [7] compared the two routing protocols of the WMNs(i.e. HWMP and RAOLSR). The research concluded that the RAOLSR routing protocol is more appropriate in cases where data traffic is distributed over the WMNs.

[8] and [9] proposed a new security enhancement mechanism by adding security features to the existing the OLSR protocol, using IBS (Identity-based signatures) technique, (i.e. HELLO and TC packets). We suggest the same HELLO and TC security package but with the Radio Aware Optimized Link State Routing protocol.

In [10], [11], [12], [13], [14] and [15], we proposed different methods in order to protect against external and internal attacks using the Radio Aware Optimized Link State Routing. In [16], we proposed the identity-based encryption (IBE) technique. We continue to expand and improve our protocol, which is designed specifically for security in the routing protocol based on the WMN. This paper compares the ECDSA-based RAOLSR against IBE-based RAOLSR protocols. In our research, we compare the Elliptic Curve Digital Signature and Identity-Based Encryption techniques in the RAOLSR protocol.

III. RAOLSR

The Radio-Aware Optimized Link State Routing protocol (RAOLSR) [1] is an optional proactive routing protocol of the Wireless Mesh Networks (WMNs). The RAOLSR is a link state layer adaptation of the Optimized Link State Routing Protocol (OLSR) [2] to the 802.11s standard. The principal difference between the OLSR and RAOLSR protocols is the use of MAC addresses instead of IP addresses. RAOLSR is an adaptation of the OLSR which reduces overhead flooding. RAOLSR frames have the format present in figure 2. The shortest route algorithm utilizes a radio-aware metric instead of the hop-count metric. Routing support for IEEE 802.11 [17] and [18] associated with mesh access points is defined. For RAOLSR a metric field is added to all topology information packets.

RA-OLSR continuously supports paths to all destinations in the WMN, which is beneficial for source and destination pairs that are very dynamic or where the WMN is large and solid. RA-OLSR is a distributed protocol without a requirement for reliable delivery of control packets.

In RAOLSR protocol, each node has two basic responsibilities. The first is that each node must correctly generate routing information and the second is that each node is responsible for reseeding packets received to other network nodes. Any alteration of these responsibilities may end up threatening the integrity of the WMNs.

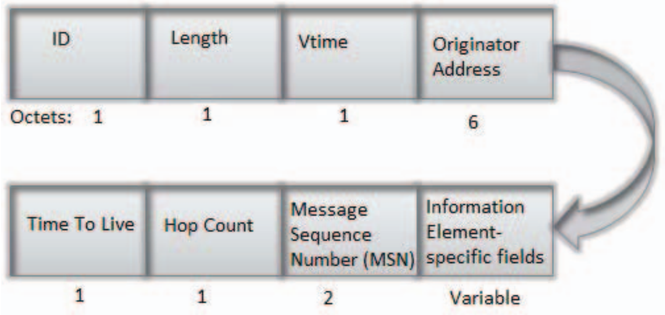

Figure 2. Format of RAOLSR information elements

IV. ECDSA and IBE

The Elliptic Curve Digital Signature Algorithm (ECDSA) [19] is the signature that can be used for the protection of routing information.

There are three procedures:

1) ECDSA key generation. Each entity A should do the following: 1. Select an elliptic curve E defined over Z^*. 2.The number of points in E(Z_p) must be divisible by a large prime number n. 3.Select a point P $\in$ E(Z_p) of order n. 4. Select an integer d statistically unique and unpredictable in the interval [1,n-1]. 5. Compute Q = dP. 6. A public key is (E, P, n, Q), the private key of A is d.
2) ECDSA signature generation. To sign an m message, A should do the following: Select a k integer statistically unique and unpredictable in the interval [1,n-1]. Compute kP=(x_1, y_1) and r=x_1 mod n. If r = 0, then return to step 1. Compute k^{-1} mod n. Compute s=k^{-1}h(m)+dr mod n, where h is the Secure Hash Algorithm (SHA). If s = 0, then return to step 1. (If s = 0 then s^1 mod n does not exist, s^1 is required in step 2 of signature verification). The signature for packet m is the pair of integers (r, s).
3) Verification of the ECDSA signature. Compute w = s^1 mod n and h(m). Compute u_1=h(m)w mod n and u_2=rw mod n. Compute R=u_1P + u_2Q = (x_0, y_0) and v = x_0 mod n. If R = O, return "invalid" and stop. Accept the signature if and only if v = r. If v$\neq$r return invalid.

Boneh and Franklins identity-based encryption scheme [20] is perhaps the most famous early example of what could be obtained using bilinear maps, though not the first. Shamir first discussed identity-based encryption [21], but researchers were unable to construct a practical scheme by conventional means for approximately twenty years. Extending the basic idea leads to identity-based schemes with additional appropriate properties, such as authenticated or hierarchical identity-based encryption and Hess [22] developed a scheme and used the identity verification, based on the survey of Boneh and Franklin [20]. This scheme has four algorithms as shown in figure 3:

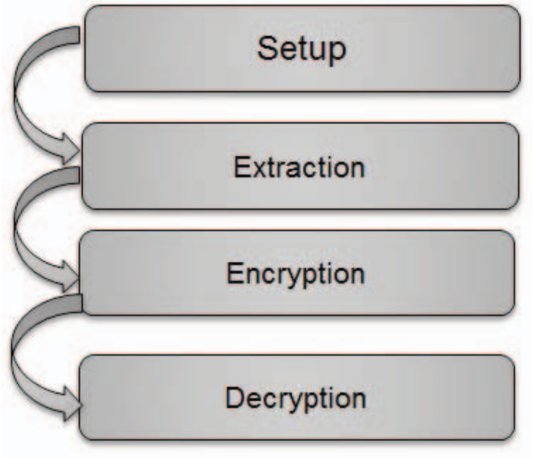

Figure 3. IBE

- **Setup:** Computes Ppub = sP and two algorithms of the following equations: For all P, Q ϵ K_1 and all c,d Z_q^*,

  $$\hat{e}(cP, dQ) = \hat{e}(cP, Q)^d = \hat{e}(P, dQ)^c = \hat{e}(P, Q)^{cd} etc \quad (1)$$

  If P is a generator of K_1, then ê(P,P) is a generator of K_2. There is an efficient algorithm to compute ê(P,Q) for all P, Q ϵ K_1
  Select a cryptographic hash function

  $$H_1 : \{0, 1\}^* \rightarrow K_1^* \quad (2)$$

  $$H_2 : K_2^* \{0, 1\}^n \quad (3)$$

- **Extract:** Apply the followings equations:

  $$Q_{ID} = H_1(ID) \epsilon K_1^* \quad (4)$$

  $$S_{ID} = sQ_{ID} \quad (5)$$

- **Sign:** Given the secret key equation, a packet is computed:

  $$C = \{rP, M \bigoplus H_2(g_{ID}^r)\} \quad (6)$$

  where

  $$g_{ID} = \hat{e}(Q_{ID}, P_{pub}) \quad (7)$$

  $$r = (\hat{e}(K_1, K_2))^n \quad (8)$$

  $$v = H(M, r)u = vS_{ID} + kP_1 \quad (9)$$

- **Verify:** Given the packet, the signature of the public key and the verification is computed:

  $$r = (\hat{e}(u, P)(\hat{(}Q_{ID}, P_{pub})))^v v = H(M, r)u = vS_{ID} + kP_1 \quad (10)$$

  and the signature is given by (u,v).

V. ECDSA-RAOLSR AND IBE-RAOLSR PROTOCOLS

The signature allows us to verify that the routing message is coming from a rightful node. Thus, a security extension can affiliate a signature to a HELLO or TC by including a digital signature in the control message.

When a node transmit a routing message, HELLO or TC message, it encrypts and authenticates the message as follows:

- First, each node must have a pair of keys, a secret private key and a published public key. These keys are generated using the ECDSA or IBE algorithm. The use of these keys protects the authenticity of a message by creating a digital signature using the private key, which can then be verified using the public key.
- Before sending a Hello or TC message, the sender node signs the Hello or TC message with its private key. The signature scheme is computed over the message header without the Time To Live and Hop-Count fields. There are certain parameters that are updated during the flooding mechanism of an RA-OLSR message.
- When a Mesh Point receives a Hello or TC message, it verifies the digital signature transmitter's public key. The TTL field of the RAOLSR message for the TC messages is used to control the scope

The vulnerabilities exist in the RAOLSR that can be exploited by the attackers to degrade the performance of the WMN. However, the security is not specified in the classical RAOLSR. We recognize some of the attacks on RAOLSR: **Incorrect generation of HELLO:** This attack is when a malicious node takes on the identity of another node. A **malicious node** takes on the identity of **4**, as shown in figure 4. Nodes **1** and **2** announce that they can reach **4** through TC and HELLO.

Another similar attack is the alteration of the links of a node, as shown in figure 5. In this case, the **malicious node** sends TC and HELLO saying that it has a link with 2 (which is not a neighbor). This impacts node 1 having an incorrect MPR Set and the messages from 3, resent through the MPRs, never reach 2.

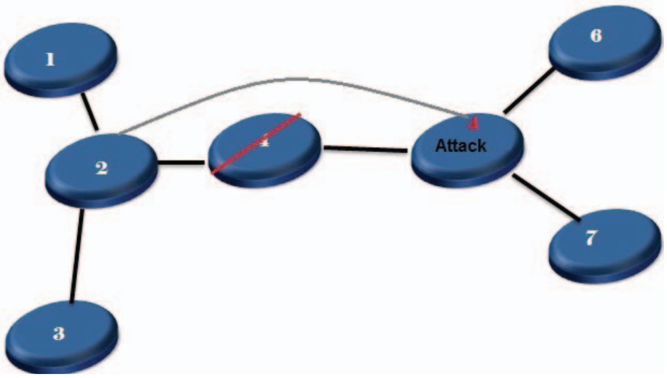

Figure 4. Identity of another

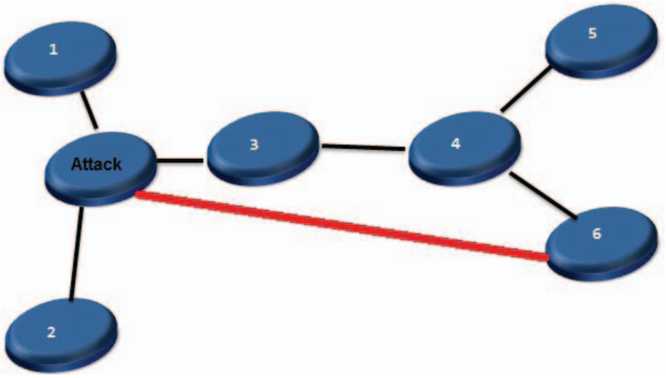

Figure 5. Modification of links

VI. PERFORMANCE EVALUATION

To integrate the IBE and ECDSA schemes in the RA-OLSR protocol, we utilize IEEE 802.11s installed at each node, the RAOLSR protocol, MIRACL library (Multi-precision Integer and Rational Arithmetic C/C++ Library) [23] and NS-3 (Network Simulator-3) [24], which contains a great number of necessary tools to design applications with cryptography. We base all our scenarios on the following parameters Table I:

A. Simulation Setup

Simulation time	200 s
Network density	1 over 80 m2
Transmission range	200 m
Bandwidth	2 Mbit/s
Node placement	Uniform
Traffic type	CBR
Packet size	512 bytes
Packet rate	10 pkts/s

Table I
PARAMETERS

In figures 6 and 7, we have compared our security protocols for WMNs with classical RAOLSR by considering the control overhead. We notice that the overhead presented by IBE-RAOLSR is not significant compared to ECDSA-RAOLSR, which is because of the benefits presented by the IBE. The reason is intuitive: establishing keys using IBE does not require negotiation between nodes. In our simulation, the key progression interval is set to five seconds, and in practice, this is adjustable according to the processing power of mobile nodes. Because shared keys between nodes need to be updated at a fixed rate, we expect that the time it takes for IBE-RAOLSR protocol to discover routes should be longer than that of ECDSA-RAOLSR protocol.

The packet end-to-end delay is the generation time of a packet by the source up to the destination node reception. Therefore this is the time that a packet takes to go across the network. This time is expressed in sec. Hence, all the delays in the network are called packet end-to-end delays for example buffer queues and transmission time. In figures 8 and 9, we also compared our considered protocols with classical RAOLSR protocol where we have computed the end-to-end delay, by considering that the maximum number of nodes is 36. Fortunately, the average routing delay caused by key progression, measured over all nodes, is only 5-12 percent more than that of RAOLSR protocol, which is acceptable. This indicates that IBE mechanism efficiently supports the security mechanisms used by the route-discovery process of IBE-RAOLR protocol without incurring significant routing delay. We observe that the IBE-RAOLSR protocol that we have added does not affect the end-to-end delay.

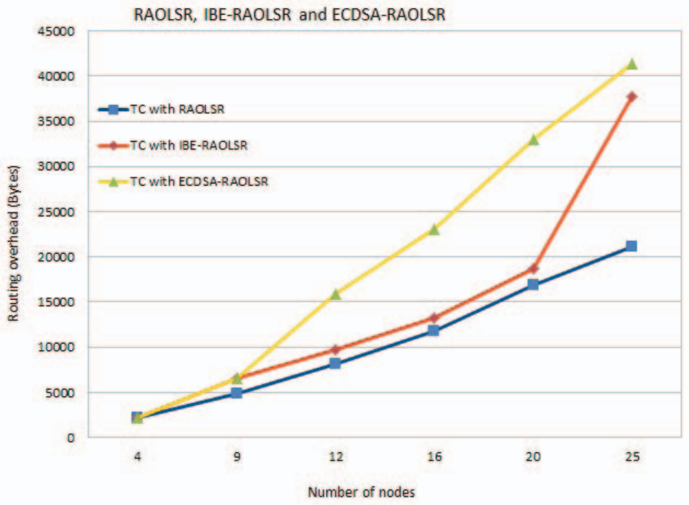

Figure 6. TC overhead: HELLO Delay: RAOLSR, IBE-RAOLSR and ECDSA-RAOLSR

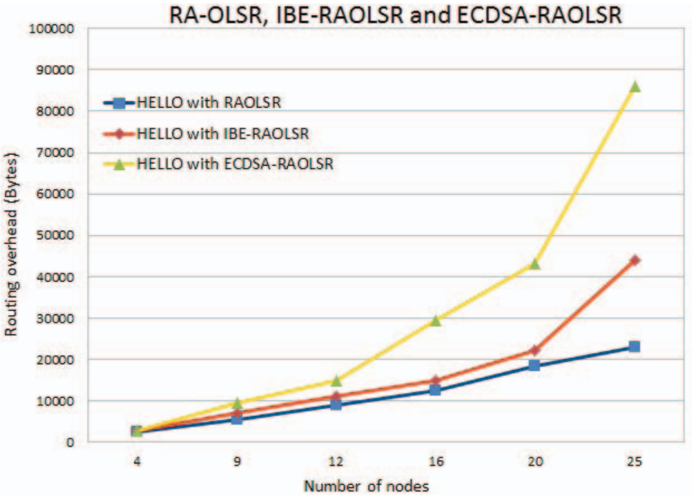

Figure 7. HELLO Overhead: RAOLSR, IBE-RAOLSR and ECDSA-RAOLSR

VII. CONCLUSION

We have implemented the IBE (Identity Based Encryption) and ECDSA (Elliptic Curve Digital Signature Algorithm) techniques to secure messages in classical RAOLSR, namely Hello and TC messages. Through simulation experiments,

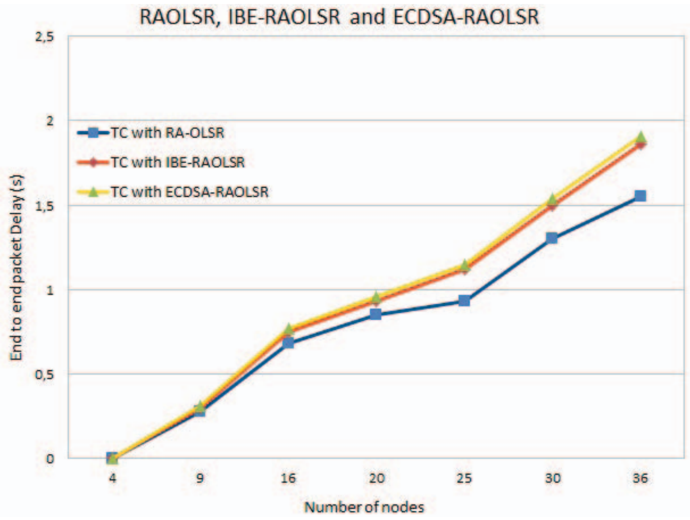

Figure 8. TC Delay: RAOLSR, IBE-RAOLSR and ECDSA-RAOLSR

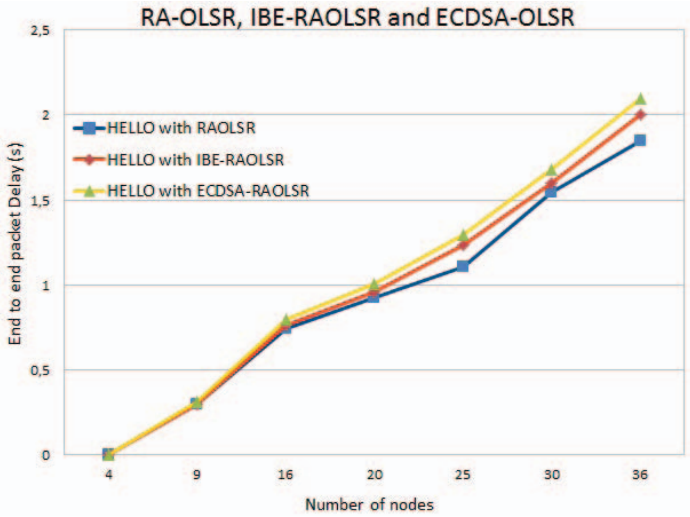

Figure 9. HELLO Delay: RAOLSR, IBE-RAOLSR and ECDSA-RAOLSR

we have evaluated the performance of our ECDSA-RAOLSR and IBE-RAOLSR in terms of delay and control overhead. Simulation results show that the ECDSA-RAOLSR does not induce a long overhead compared to the classical RAOLSR protocol. This study shows the great benefits of the IBE technique in securing RAOLSR. Through extensive Network Simulator-3 simulations, results have shown that the IBE-RAOLSR outperforms the ECDSA-RAOLSR in terms of overhead and delay. Simulation results show that the use of the IBE-based RAOLSR provides a greater level of security with light overhead.

In future work, we intend to simulate trust management in the classical RAOLSR protocol.

References

[1] IEEE P802.11s/D4.0 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 10: Mesh Networking (December 2009)

[2] Jacquet P. et al., Optimized Link State Routing Protocol for Ad Hoc Networks. In Proc. INMIC 2001, 2001.

[3] Guangyu Pei, Gerla, M. and Tsu-Wei Chen. Fisheye state routing: a routing scheme for ad hoc wireless networks. Proceedings of IEEE ICC, 2000, New Orleans, LA, pp. 70 - 74 vol.1.

[4] P. Chatzimisios, A.C. Boucouvalas and V. Vitsas, Optimisation of RTS/CTS handshake in IEEE 802.11 Wireless LANs for maximum performance, in Proceedings of the IEEE Global Telecommunications Conference (Globecom 2004) Workshops, pp. 270-275, Dallas Texas, USA, 2004.

[5] A. Sgora, D. D. Vergados and P. Chatzimisios, IEEE 802.11s Wireless Mesh networks: Challenges and Perspectives , in Proceedings of the 1st International Conference on Mobile Lightweight Wireless Systems (MOBILIGHT 2009), Athens, Greece,18-20 May 2009.

[6] Ulrich Herberga, Thomas Clausen, and Milan, J.; Digital Signatures for Admittance Control in the Optimized Link State Routing Protocol Version 2. Internet Technology and Applications. Pages. 1-4. 2010.

[7] Ghannay, S.; Gammar, S.M.; Kamoun, F. Performance comparison of hop count and radio aware path selection protocols in IEEE 802.11s WLAN mesh networks. Wireless Days, WD '08. 1st IFIP. pp. 1 - 5. 2008.

[8] A. M. Hegland, P. Spilling, L. Nilsen, and O. Kure. Hybrid Protection of OLSR. Workshop on Cryptography for Ad-hoc Networks (WCAN06). 2006.

[9] Mona Holsve Ofigsb. Anne Marie Hegland, Pl Spilling, ivind Kure and Leif Nilsen. Scalable Revocation in Hybrid Ad Hoc Networks. The SHARL Scheme. JOURNAL OF NETWORKS. VOL. 3, NO. 6. JUNE 2008.

[10] J. Ben-Othman and Y. I. Saavedra Benitez. On Securing HWMP using IBC. International Conference in Communications (ICC2011). Pages:1-5. June 5-9. 2011. Kyoto, Japan.

[11] J. Ben-Othman and Y. I. Saavedra Benitez. IBC-HWMP: a novel secure identity-based cryptography-based scheme for HWMP for IEEE 802.11s. Journal of Concurrency and Computation: Practice and Experience, DOI: 10.1002/cpe.1813 Published on: 19 August 2011, Publisher John Wiley and Sons Ltd. Chichester, UK 2010.

[12] J. Ben-Othman, L. Mokdad and Y. I. Saavedra Benitez. Performance Comparison Between IBC-HWMP and Hash-HWMP", in the Proceedings of the IEEE Conference on Global Telecommunications (GLOBECOM 2011). Pages: 67-71. 5-9 December 2011. Houston, TX, USA.

[13] J. Ben-Othman and Y. I. Saavedra Benitez. A light weight security scheme for HWMP protocol using Elliptic Curve technique", Full paper track, in the Proceedings at the 34th Annual IEEE Conference on Local Computer Networks (LCN 2011), Pages: 850-854, during the period 4-7 October 2011, Bonn, Germany.

[14] J. Ben-Othman, J.P. Claude and Y. I. Saavedra Benitez. A Novel Mechanism to Secure Internal Attacks in HWMP Routing Protocol. IEEE International Conference in Communications (ICC2012). Pages:162-166. June 10-15 2012, Ottawa, Canada.

[15] Y. I. Saavedra Benitez, J. Ben-Othman and J. P. Claude. Performance Comparison between IBE-HWMP and ECDSA-HWMP. Journals Production Department, Security and Communication Networks. Published on: 19 August 2011, Publisher John Wiley and Sons Ltd. Chichester, 2012.

[16] J. Ben-Othman, and Y. I.Saavedra Benitez, A new Method to Secure RA-OLSR using IBE, Global Telecommunications (GLOBECOM2012). California, USA. 2012.

[17] D. Takahashi, Y. Xiao, Y. Zhang, P. Chatzimisios and H.-H. Chen, IEEE 802.11 User Fingerprinting and Its Applications, Elsevier Computers and Mathematics with Applications, Vol. 60, Issue 2, pp. 307-318, 2010.

[18] Petros Spachos, Periklis Chatzimisios and Dimitrios Hatzinakos, Energy Efficient Cognitive Unicast Routing for Wireless Sensor Networks, accepted (to appear) in Proceedings of the IEEE Vehicular Technology Conference (VTC 2013), Dresden, Germany, June 2013.

[19] Don Johnson and Alfred Menezes and Scott Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA), International Journal of Information Security, Volume 1, Number 1. Pages 36-63, August. 2001.

[20] D. Boneh and M. Franklin. Identify-based Encryption from The Weil Pairing, Crypto01. Pag. 213- 219, 2001.

[21] Adi Shamir. Identity Based Cryptosystems and Signature Schemes. Proceeding of Crypto 1984, pp. 47-53. 1984.

[22] Florian Hess. Efficient identity based signature schemes based on pairings. Workshop on Selected Areas in Cryptography, pages 310-324, London, UK, 2003.

[23] Michael Scott. MIRACL. Shamus Software Ltd, Dublin, Ireland 2003.

[24] The Network Simulator 3: http ://www.nsnam.org