Security Ontology for Semantic SCADA

Sahli Nabil, Benmohamed Mohamed

(LIRE) Distributed Computer Science Laboratory
Mentouri Constantine University & SONELGAZ Group
Po.Box 325, Route Ain El Bey 25017 Constantine Alegria
n.sahli@sonelgaz.dz, ben_moh123@yahoo.com

Abstract. Web services have become a significant part of embedded systems as SCADA and internet applications embedded in RTU, because (WS) was XML/SOAP support, independent to platform and very simple to use, these advantages make (WS) vulnerable to many new and old security attacks. Now, it becomes easier to attack (WS) because their semantic data is publicly accessible in UDDI registry and (WS) use http protocol and the 80 TCP port as an open tunneling as a very big vulnerability. We work for the development of better distributed defensive mechanisms for (WS) using semantic distributed (I/F/AV) bloc, security ontology's and WS-Security framework accelerated by ECC mixed coordinates cryptography integrated in our global security solution.

Keywords: SCADA; Web Services (WS); IDS/Firewall/Antivirus (I/F/AV) bloc; ECC Cryptography; Security Ontology.

1 Introduction

The XML Web services open 70% of root for the hackers that firewall and IDS can't detect [2]. Hackers can transport all data with the 80 port, and firewall can't detect this attack [2]. With HTTP protocol Web services can destroy the security strategy the 80 port is always open because it is used by the HTTP protocol used by the web navigators, to create a tunneling, became a very big vulnerability. One of the key challenges to successful of the integration Web services technologies in the embedded system and the SCADA RTU (Remote Terminal Unit) is how to address crosscutting architectural concerns such as policy management and security, governance, authentication, a hacker's attacks, semantic attack and traditional attack.

To address this challenge, this article introduce the notion of semantic attacks in SCADA RTU using the semantic information in the UDDI registry and security concerns lead to the enhancement of SOAP messages via WS-Security framework. In our research, we work to secure the semantic and intelligent Web services embedded in the SCADA RTU, as presented in the figure 1.

We present in this article our approach of accelerating and optimizing security ontology with mixed coordinates ECC cryptography. We begin our article with

presenting SCADA platform used in our research, after that we present security of semantic web services embedded in SCADA RTU, then we present a modified semantic Mitnick attack, after that we present our ontology based semantic distributed (I/F/AV) bloc for SCADA, also we present our solution for optimizing WS-Security framework with mixed coordinates ECC for complex embedded system as SCADA, finally we conclude with a conclusion and our future work and perspectives in our research.

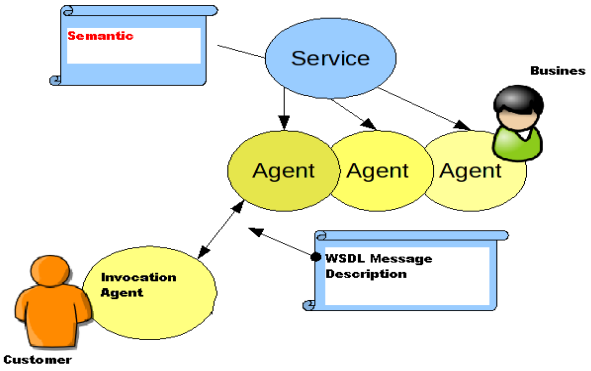


Fig1. Intelligent and semantic Web services embedded in SCADA RTU

2 SCADA Platform Used In Our Research

We use the first IP-based RTU solutions that enable complete integration of SCADA, control, and communications functionality in one rugged package. Our simple yet powerful products leverage easy-to-use Web technologies and inexpensive public networks. They are easy to configure and offer dramatically reduced costs versus traditional SCADA/PLC systems as presented in the figure 2.

Fig 2. Web services and XML technologies embedded in the SCADA RTU [25]

The SCADA RTU integrate, internet compatibility, E-mail messaging, SMS text messaging, Web pages served via the internet or intranets, using FTP file transfer as (CSV,JPEG, etc.), Embedded internet and Web server text messaging, SCADA compatibility with protocols (MODBUS, DNP3,…etc), SCADA protocol messaging to host computer system, multi communications include (Ethernet, RS-232, RS-485, Fiber optics, GSM/GPRS, PSTN modem, private line modem, and radio) each port operates independently of each other, programmable control, alarm management, data logging and intelligent end device compatibility as (sensors, actuators, digital and intelligent camera, electronic metering devices and process inputs/outputs (fixed and mobile assets as filters, generators, motors, pumps, valves)), as presented in the figure 3.

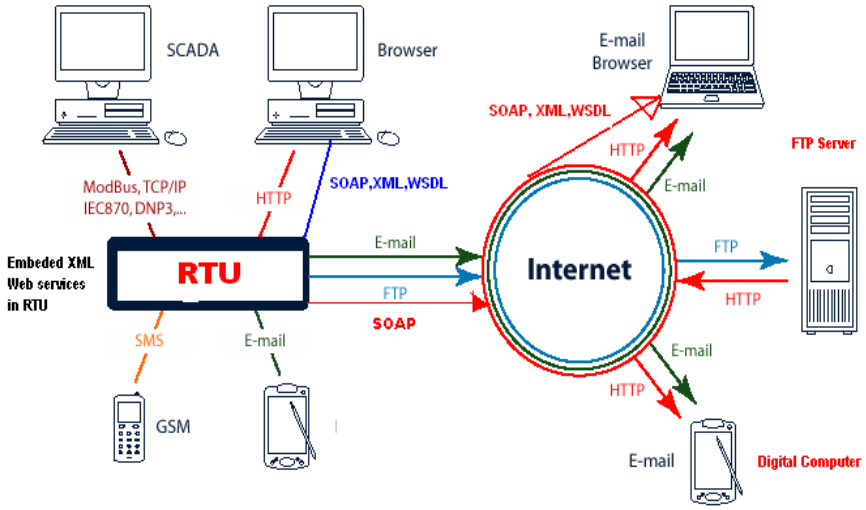


Fig3. SCADA platform and protocols used in our research

For critical applications as SCADA in energy networks security and monitoring, communications redundancy is supported. The RTU SCADA used in Algerian Ministry of Energy and Mining offer an ultra-compact OEM solution, it can be rapidly adapted to many embedded applications and can be connected to the internet for worldwide monitoring, can be served to internet portals regularly or upon events.

3 Security of Semantic Web Services Embedded In SCADA RTU

Semantic (WS) have raised many new unexplored security issues as new ways of exploiting inherit old security threats, semantic (WS), which can publish the information about their functional and non-functional properties, add additional security threats. The hackers do not need to scan the Web and SCADA network to find targets. They just go to UDDI Business Registry in the SCADA control room and get all the information's they need to attack semantic Web services. Now, the whole semantic (WS) attack consists of several stages during which a hacker discovers weakness, then penetrates the semantic (WS) layer and gets access to SCADA critical applications and infrastructures.

For example, the XML Injection attack [7] occurs when user input is passed to the XML stream, it can be stopped by scanning the XML stream. Another type of attacks on (WS) is Denial of Service (DoS) attack when attackers can send extremely

complicated but legal XML documents, it forces the system to create huge objects in a memory and deplete system's free memory. Distributed and multi-phased attacks such as the Mitnick attack [8] are more dangerous for semantic (WS) embedded in the SCADA RTU because IDS [9, 18] can detect them only by acting as a coalition with firewall as a semantic bloc. We need antivirus in the coalition bloc for other kind of vulnerability as distributed and mobile virus. Semantic (WS) embedded in the SCADA RTU are vulnerable at a lot of attacks as: (Application Attacks, Discovery attacks, Semantic Attacks, SOAP Attacks, XML Attacks ….etc.), as presented in the figure 4, in the following subsections.

The attacker begin by finding Web services using UDDI registry, after that he discover points of weakness in WSDL documents which can be used as a vulnerability guide book for getting access to SCADA RTU critical applications and infrastructures, and create a lot of damages as different kind of semantic Web services attacks: Discovery Attacks [12], WS DoS Attacks [7], CDATA Field Attacks [7], SOAP Attacks [12], Application Attacks [7] [9] [10] [11], XML Attacks [7], Semantic WS Attacks [7]

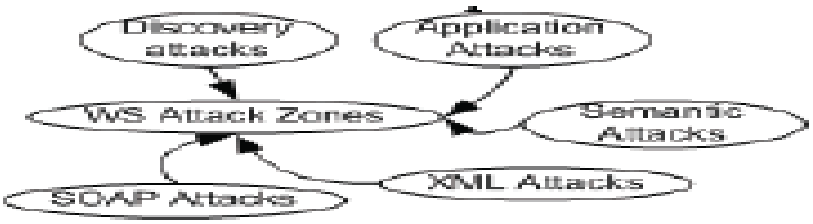


Fig. 4. Attack Zones [12]

4 Modified Semantic Mitnick Attack

The Mitnick attack step is presented in the figure 5 below.

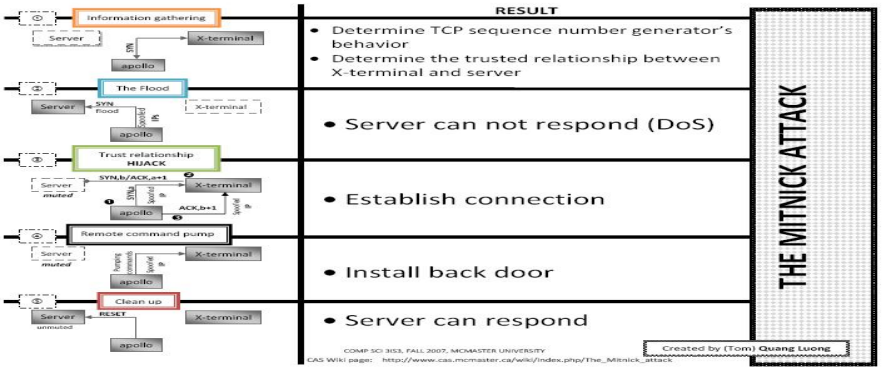


Fig .5. The Mitnick attack Steps [22]

The Mitnick attack can be modified for using in conjunction with the XML Injection attack, semantic (WS) Mitnick attack is organized as follows:

1. An **Attacker** navigates to UDDI registry and asks for a service (Gas temperature) for example.
2. The **Attacker** attaches to UDDI and asks for WSDL files.
3. For blocking communications between **Host1** and **Host2**, **Attacker** starts a Syn/Flood attack against **Host1**.
4. **Attacker** sends multiple TCP packets to **Host2** in order to predict a TCP sequence number generated by **Host2**.
5. **Attacker** pretends to be **Host1** by spoofing **Host1**'s IP address and tries to establish a TCP session between **Host1** and **Host2** by sending a Syn packet to **Host2** (the **Step 1** of a three way handshake).
6. **Host2** responds to **Host1** with a Syn/Ack packet (**Step2** of a three way handshake), however, **Host1** cannot send a RST packet to terminate a connection because of a Syn/Flood (Dos) attack from Step3.
7. **Attacker** cannot see a Syn/Ack packet from Step 6, however, **Attacker** can apply a TCP sequence number from Step4 and **Host1**'s IP address and send a Syn/Ack packet with a predicted number in response to a Syn/Ack packet sent to **Host1** (**Step 3** of a three way handshake).
8. Now, a **Host2** thinks that a TCP session is established with a trusted **Host1**. **Attacker** can attack **Host2** semantic Web services that believe that has a session with **Host2**.
9. **Attackers** inspects **Host2** WSDL files in order to find dangerous methods.
10. **Attacker** tests these methods in order to find possibilities for the XML Injection attack.
11. **An attacker** applies XML Injection for changing Attacker's ID and getting more privileges.
12. If the XML Injection attack is not successful **Attacker** can try the SQL Injection attack or any other injection attacks as XPATH attack or others, against semantic Web services because **Host2** still believes that it is connected to **Host1**.

Our OWL class for the modified Mitnick attack is shown as follows:

```
<owl :Class rdf :ID= '&WSAttacks ;WSMitnick'>
 <owl: intersectionOf rdf: parseType="Collection">
  <owl:Class rdf:about="#Probing"/>
  <owl:Class rdf:about="#WSProbing"/>
  <owl:Class rdf:about='#SynFlood"/>
  <owl:Class  rdf:about="#XMLInjection"/>
 </owl:intersectionOf>
</owl:Class>
```

To detect the modified Mitnick attack, the distributed bloc (I/F/AV) installed in the network between Host1 and Host2 should operate as a coalition using the security attack ontology based on distributed (I/F/AV) bloc cooperation, in SCADA systems Host1 must be client and Host2 the RTU.

5 Our Ontology Based Semantic Distributed (I/F/AV) Bloc for SCADA

Using Ontology for creating distributed defenses using IDS [17] is introduced in [8], but, it takes into account only application attacks. A lot of security ontology's of Web services are described in [19], describes types of security information including security mechanisms, objectives, algorithms, credentials and protocols using security ontology's as SWSL[3], WSMO [4], KAoS[5], METOR-S[6], OWL-S [20]. It's applied to SOA to show how Web services can publish their security requirements and capabilities. Security properties and security policies of Web services must be expressed in SCL [14, 15, 16], as automatic reasoning. Our security threats of embedded semantic Web services in SCADA RTU and our proposed defense techniques based distributed semantic (I/F/AV) bloc presented in the figure 6 bellow using VPN Tunneling security technique (VPN1 for ERP and information system and VPN2 for SCADA system), Packet Filtering and Port Filtering.

As shown in the table 1, Web services are generally modeled as resting on top of TCP/IP application protocols such as HTTP. For securing embedded Web services in SCADA RTU we use protocols as (HTTPS, IPSEC, SSL) and other techniques as content filtering and a mixed coordinates ECC encryption with (affines, Montgomery and jacobian) coordinates.

Our Security solution for embedded semantic (WS) uses standards as (OWL/OWL-S) [21, 20], for more detail read [11, 14]. We use WS-Security framework (XML Signature, XML Encryption, WS-Security, WS-SecureConversetion equivalent as SSL in SOAP level, WS-Trust, WS-Federation, WS-Policy and WS-SecurityPolicy,

WS-Privacy for management of confidentiality politic with the use of jetton and WS-Authorization) as specified in the figure 7.

Our security solution uses WS-Security framework as presented in the figure 8, our solution include all XML security techniques as transforming, caching, ECC encryption and decryption, auditing, logging, screening and filtering, verification, validation, authentication, authorization, and accounting.

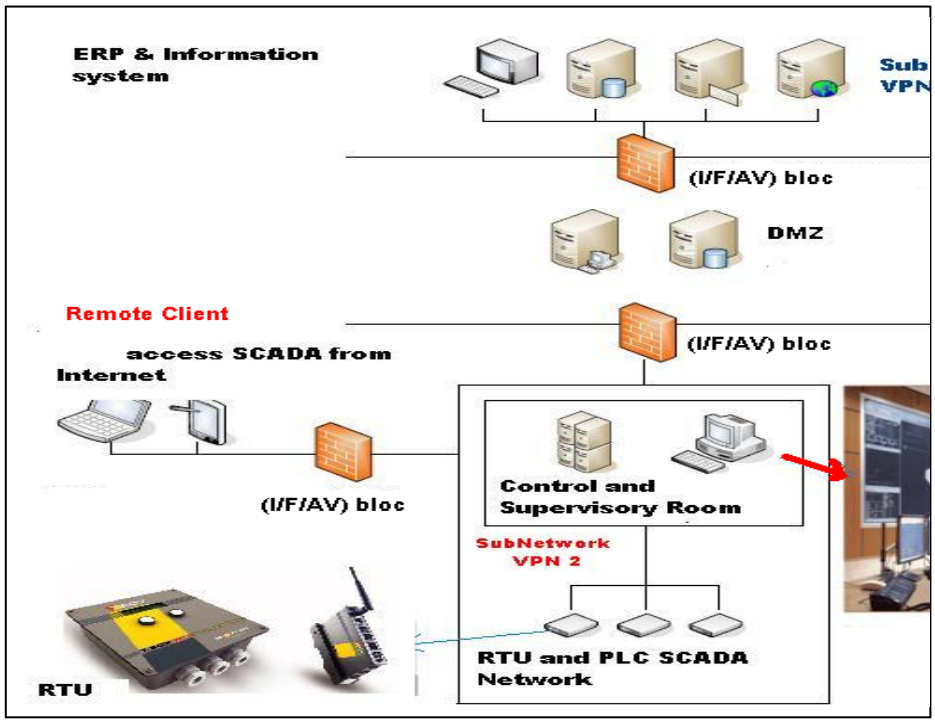


Fig. 6. Our security solution Platform for SCADA

Network Layer	Protocols	Security Technique
Application	HTTP, HTTPS	Content Filtering & ECC Encryption (a **mixed** of affine, Montgomery and Jacobian **coordinates) & SSL Protocol**
Transport	TCP, UDP	Port Filtering
Inter network	IP, ICMP	Packet Filtering & IPV6
Data Link	PPTP, L2TP	VPN Tunneling (VPN1 & VPN2)

Table 1. Security techniques proposed for SCADA systems

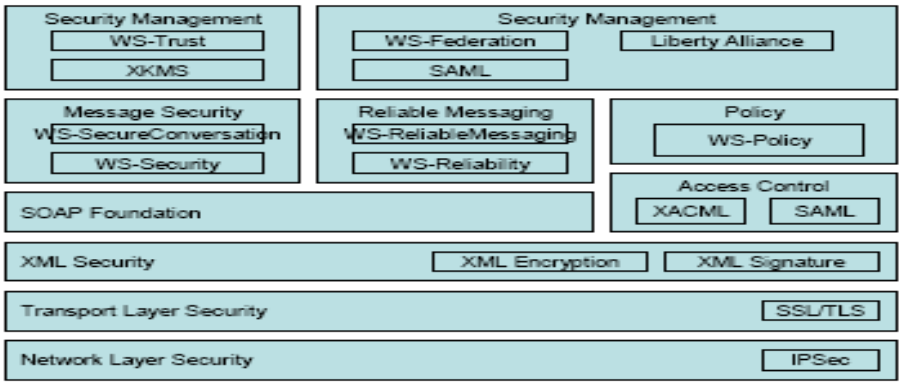


Fig.7. WS-Security framework stack [1] [13]

Our solution use ten (10) steps as : message signature operation, message crypt operation, associating a jetton in the SOAP message (steps : 1,5) and the SOAP message preparation (step 4) in distance customer, and SOAP message transmission (step 7), validation operations , decrypting SOAP messages and to certificate them (steps: 8,9,10) in SCADA RTU, also the Service Registry, Policy Store and Identity Provider (steps :2,3,6) , as presented in the figure 9.

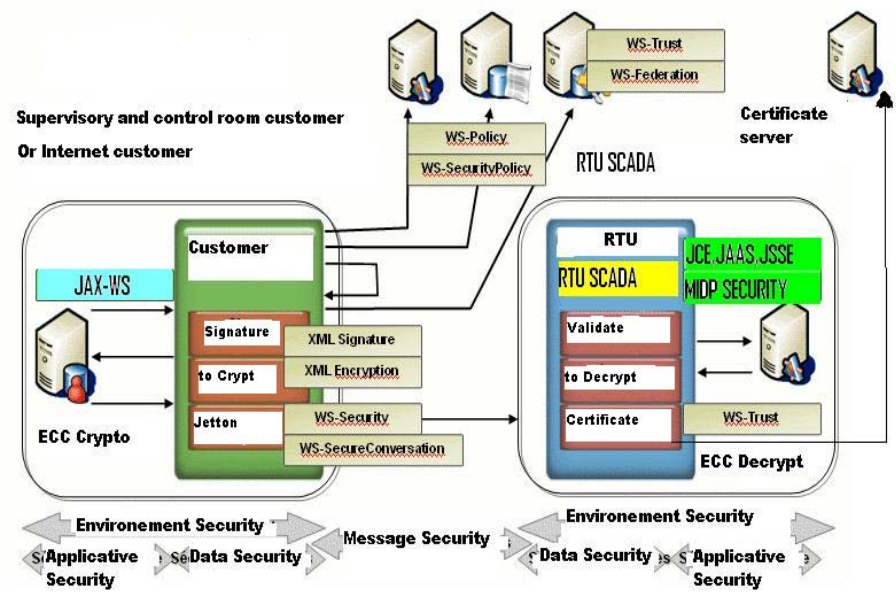


Fig. 8. Our Security solution for SCADA

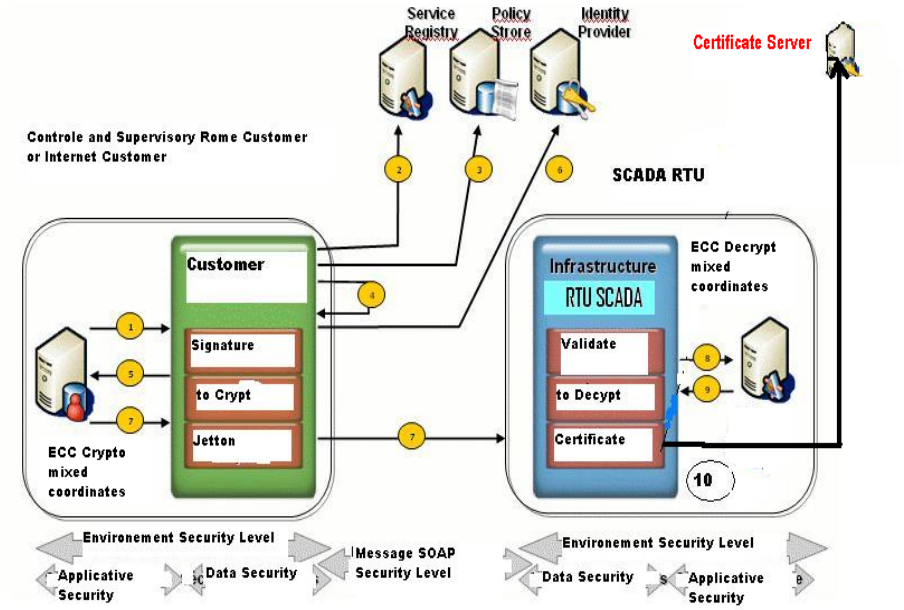
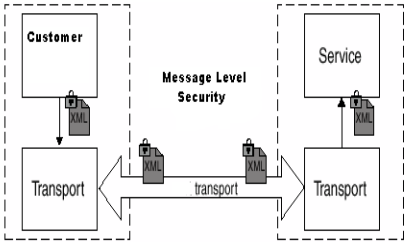


Fig.9. The Ten (10) steps of our security solution for SCADA

Our solution includes a lot of security levels as (applicative security, data security, environment security and message SOAP security). We present in the figure 10 and 11 our SOAP message security proposed solution.



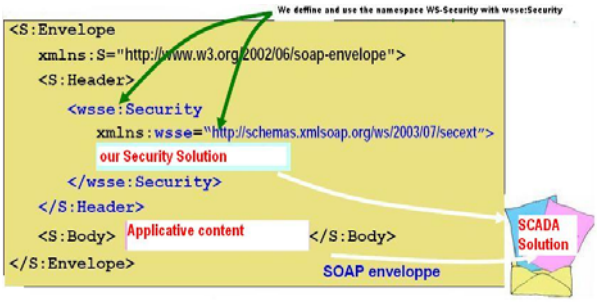


Fig.10. A SOAP security message solution Fig.11. SOAP message security implemented in RTU

6 Optimizing WS-Security Framework with Mixed Coordinates ECC

Elliptic curve cryptography (ECC), independently introduced by Koblitz and Miller in the 80's [27], has attracted increasing attention in recent years due to its shorter key length requirement in comparison with other public-key cryptosystems such as RSA. Shorter key length means reduced power consumption and computing effort, and less storage requirement, factors that are fundamental for SCADA systems as presented in the figure 12. Comparing (WS) secured by WS-Security framework to unsecured Web services, the WS-Security is by factor 100 slower than Web services. WS-Security should be used only where security has the highest priority over performance, but it is not the case of the embedded complex system as SCADA system and embedded Web services in the SCADA RTU. Our approach is to optimize WS-Security framework by using our solution based mixed coordinates ECC [24] for the operations (to crypt, to decrypt, to sign and to verify signature) SOAP messages as presented in our solution figures 8 and 9.

Algorithme	Size of Key (bits)	Signature		Vérification	
		Time (s)	Energy consumption (mW)	(s)	Energy consumption (mW)
RSA	1024	22.03	726.99	0.86	28.38
RSA	2048	166.85	5506.05	3.89	128.37
ECC	160	1.65	54.45	3.27	107.91
ECC	224	4.46	174.18	8.84	291.72

Fig. 12. ECC and RSA comparative [26]

Our analyze in the database « **Explicit-Formulas Database** » [23] determine the result shown below in Figure 13 and 14.

Coordinats	Addition	Doubling	Mixed Addition
Modifiees	13M+6S	4M+4S	-
Brier & Joye	9M+2S	6M+3S	-
Montgomery	4M+2S	**3M+2S**	-
Affines	**I+2M+S**	I+2M+2S	-
Projectives	12M+2S	7M+5S	9M+2S
Jacobiennes	12M+4S	4M+6S	**7M+4S**
Chudnovsky	11M+3S	5M+6S	-

Fig. 13. Cost of ECC coordinates in the field Fp

Coordinats	Addition	Doubling	Mixed Addition
Affines	**I+M**	**I+M**	-
Projectif (c=1, d=1)	13M	7M	12M
Jacobien	14M	5M	10M
Lopez-Dahab	14M	4M	**8M**

Fig.14. Cost of ECC coordinates in the field $F2^m$ (**M**: Multiplication, **S**: square, **I**: Inversion)

Our ECC optimized algorithm « **Mixed-Coordinates-ECC-Algo** » is presented below:

1. We compute the doubling operations with « Montgomery » coordinates for preparing the addition operation in the field Fp and with « Affines» coordinates for the field $F2^m$.
2. We compute the addition of the last point computed and another point in the curve, with « Affines » coordinates, for the two fields Fp and $F2^m$.
3. All addition operation will be computed with « Affines » coordinates for the two fields Fp and $F2^m$.
4. All mixed addition operation will be computed by « Lopez-Dahab » coordinate for the field $F2^m$ and « Jacobiennes » coordinates for the field Fp.

7 Conclusion

The SCADA RTU including embedded Web services and embedded XML creates a new big challenge in security for SCADA, because network security is maturing and semantic embedded Web services security not mature. Specific procedures for securing embedded XML SCADA network applications are not yet widely known. We present our security solution introduced in this paper for embedded SOA security design, with a distributed implementation of a distributed semantic bloc (I/F/AV) between client and RTU. Our approaches is composed with ten (10) steps using ECC mixed coordinates cryptography solution and WS-Security framework, adapted and optimized for SCADA systems. We use a bloc of products such XML semantic firewalls, proxies, IDS, gateways, VPN technologies, security protocols (HTTPS, IPSEC, and SSL), a security framework as WS-Security and ECC mixed coordinates cryptography integrated in our solution. We propose a security solution of semantic Web services embedded in RTU using security ontology's as OWL/OWL-S. We work to do more optimization and to implement our solution with a real material used in Algerian ministry of energy and mining as TBOX RTU manufactured by CSE-Semaphore Group Company [25] and TOSSIM (PowerTossim & TinyViz) simulator [28].

References

1. Aymen BOUGHATTAS & Med Aymen BAOUAB, Web service security (WS-Security), a master degree memory 2008/2009 Nancy Franch University, 2009.

2. Soaj2ee.blogspirit.com/files/whitepaper/soaj2ee-security-transport.pdf

3. SWSL, http://www.daml.org/services/swsl/

4. WSMO, http://www.wsmo.org/

5. KAoS. http://www.ihmc.us/research/projects/KAoS/

6. METEOR-S, http://lsdis.cs.uga.edu/projects/meteor-s/

7. A.Stamos and S.Stender, "Attaking Web Services: The Next Generation of Vulnerable Entreprise Apps, BlackHat2005, USA, 2005.

8. J.Undercoffer, A.Joshi, T.Finin, and J.Pinkston, A target-centric ontology for intrusion detection, Int, Joint Conference on Artificial Intelligence, Mexico, 2004.

9. J.Mirkovic, "D-WARD: Source-End Defence Against Distributed Denial-of-Services Attacks", The Phd thesis, University of California, 2003.

10. P.Lindstrom, "Attacking and Defending Web Services", A Spire Research Repport, January 2004.

11. W.Negm, "Anatomy of a Web Services Attack: A Guide to Threats and Preventive Countermesures", 2004.

12. S.Faut, "SOAP Web Services Attacks: Are you web applications vulnerable", SPI Dynamics,2003.

13. T.Erl, "WS-* Specifications, An Overview of the WS-Security Framework", 2004.

14. K.Khan and J.Han, "A Security Characterisation Framework for Trustworthy Component Based Software Systems",COMPSAC2003, USA,2003.

15. A.Vorobiev and J.Han, "Specifiying Dynamic Security Properties of Web Service Based Systems", SKG2006,Guilin, China,2006.

16. K.Khan, "Security Characterisation and Compositional Analysis for Component-based Software Systems", PHD thesis, Monash University, April 2005.

17. S. Axelsson, "Research in Intrusion-Detection Systems: A Survey, Technical report 98-17, Chalmers University of Technology, 1998

18. G. Denker, S.Nguyen, and A.Ton, OWL-S Semantics of Security Web Services: a Case Study, SRI Internayional, Menlo Park, California, USA, 2004

19. A.Kim, J.Luo, and M.Kang, Security Ontology for Annotating Ressources, ODBASE 2005, Cyprus, 2005.

20. OWL-S: Semantic Markup for Web Services, November 2004,

http://www.w3.org/Submission/OWL-S/

21. OWL, http://w3.org/TR/owl-features/

22. http://wiki.cas.mcmaster.ca/index.php/The_Mitnick_attack

23. http://www.hyperelliptic.org/EFD/ Explicit-Formulas Database

24. H. Cohen, A. Miyaji, and T. Ono. Efficient elliptic curve exponentiation using mixed coordinates. In ASIACRYPT, LNCS. Springer, 1998.

25. CSE-Global group company, europe Belgium www.CSE-Semaphore.com

26. A.Patel, Arvinderpal Wander, Hans Ebele, Sheulling C hang Shantz, comparing elliptic curve cryptography and RSA on 8-Bit CPUs,2004.

27. N. Koblitz. A Family of Jacobians Suitable for Discrete Log Cryptosystems. In Shafi Goldwasser, editor, Advances in Cryptology - Crypto ’88, volume 403 of Lecture Notes in Computer Science, pages 94 – 99, Berlin, 1988.

28. Victor Shnayder, Mark Hempstead, Borrong Chen, Geoff Werner Allen, and Matt Welsh, Simulating the Power Consumption of LargeScale Sensor Network Applications, Harvard University, Baltimore, Maryland, USA, *SenSys’04,* November 3–5, 2004.