Ibn Al-Haitham Journal for Pure and Applied Science | مجلة إبن الهيثم للعلوم الصرفة و التطبيقية
No. 1 Vol. 25 Year 2012 | العدد 1 المجلد 25 السنة 2012

Lagrange Interpolation for Mobile Agent Connection Encryption

H. K. Homood
Department of Computer Science, College of Education, University of Al-Mustansirya

Received in:6June2011, Accepted in:13July2011

Abstract

A new proposed technique for secure agent communication is used to transfer data and instructions between agent and server in the local wireless network. The proposed technique depends on the two stages of encryption processing (AES algorithm and proposed Lagrange encryption key generation supported by XOR gate) for packets encryption. The AES key was manipulated by using proposed Lagrange interpolation key generated in order to avoid the weak encryption keys. A good multi encryption operation with a fast encryption time was proposed with a high quality connection operation.

Keyword: Agent, Agent security, Mobile Agent, Lagrange interpolation application.

Introduction

Mobile agents are goal-directed, autonomous programs capable of migrating from host to host during their execution. The combination of autonomy and mobility provides mobile agent's enormous potential for application in today's Internet-based, distributed computing environment. Typical application areas, to name a few, include E-commerce, information retrieval, software distribution administration, and network management.

Trust is little trust in a typical Internet application between the originator and the hosts, and neither the hosts trust each other. Security threats are therefore considered against the two main targets: either threats against the hosts, or threats against the agent, which represent the interests of the originator.[1]

The current developments of computer systems are leading to a situation where the number of processors and computer networks is becoming more and more pervasive. Nowadays, there are processors embedded in lots of everyday devices. From personal computers, laptops, PDAs, and mobile phones, to refrigerators, heaters, coffee machines, or toasters. Furthermore, these devices can be interconnected through computer networks. The increased research on wireless and mobile networks is making possible to have cheap networks at home, at the office or even at the streets.[2]

Wireless communications offer organizations and users a lot of benefits. Portability and flexibility, increased productivity, and lower installation costs are just few of wireless communication benefits. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs. Ad hoc networks, such as those enabled by

Bluetooth, allow data synchronization with network systems and application sharing between devices.[1]

Knowing what kind of individual might launch an attack against your wireless network is just as important as being aware of his or her motivations. From the motivations already outlined, it is possible to split attackers of wireless networks into three main categories:[3]

- Curious individuals who do it for both fun and the technical challenge. This category of attackers does not usually present a huge threat to your WLAN and might even do a service to the community by publicly exposing insecure wireless networks and raising public awareness of wireless security issues. Many of them could actually become (or already are) wireless networking professionals and security tools developers for the Open Source community.[3]
- "Bandwidth snatchers." This category of wireless crackers is the "script kiddies" of the wireless world. Spammers and "warez" / pornography traders as well as some "I like my neighbor's wireless" opportunistic types belong here. They usually go for the lowest hanging fruit and are easy to repel (even WEP and MAC address filtering might do, but don't be so sure).[3]
- Real Black Hats who happen to like wireless. These are the serious attackers who generally know what they do, why they do it, and what the legal consequences could be. Anonymity, lateral attacks on otherwise protected networks, and out-of-band backdoor access are the reasons professional crackers are attracted to wireless networks. Standard security measures will only delay such attackers by a couple of hours. Unless the security of the 802.11 network is given proper attention in both time and effort, the attack will inevitably succeed.[3]

However, risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. Perhaps the most significant source of risks in wireless networks is that the technology underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot.[1]

While the Bluetooth functionality is also eliminates cables for printer and other peripheral device connections. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders.[1]

In this paper, we present a new technique for agent connection make more secure in wireless network using a proposed Lagrange interpolation polynomial calculations to generate robust keys for AES (128bit) encryption algorithm and to encrypt/decrypt the sending/ receiving data through the wireless network. These approaches will increase the security of transfer data between the agents and center agent server.

1. Mobile Agent

Mobile Agent is a composition of computer software and data which is able to migrate (move) from one computer to another autonomously and continue its execution on the destination computer. [1]

As the definition says, a mobile agent moves both code and data to the destination machine. The agent executes the migrated code under the runtime environment provided by the target machine. The agent can share the migrated data with the local machine and acquire new data from it. This can be done only under the security privileges that the agent possesses on the target machine. However, the agent is free to communicate to another locally running agent on the target machine. Illustrated in figure 1 is the use of local stationary mobile agent as a mediator between the visiting mobile agent and the local resources.

In recent years, several programming languages for mobile agents have been designed. These languages make different design choices as to which components of a program state can migrate from machine to machine. [1]

2. Infrastructure for Mobile Agents

As computational processes, agents do not exist on their own but rather within computing software and hardware providing them mechanisms to execute. Many agent implementations also require substantial libraries and code modules. Further, agents frequently possess properties not found in traditional software, such as mobility. Development and implementation of such software requires significant infrastructure to provide core functionality agents may use in conducting their tasks. [4]

An agent-based system comprises one or more agents designed to achieve a given functionality, along with the software and hardware supporting them. It is comprised of several layers as shown in Figure 1 and described as follows: [4]

- Agents implement the application; they achieve the intended functionality of the system.
- Frameworks provide functionality specific to agent software, acting as an interface or abstraction between the agents and the underlying layers. In some cases, the framework may be trivial or merely conceptual. For example if it is merely a collection of system calls or is compiled into the agents themselves. At one extreme, the framework could even be considered "null" or empty, such as in the case where agents are programmed directly into hardware.
- Platforms provide more generic infrastructure from which frameworks and agents are constructed and executed. Items such as operating systems, compilers, and hardware drivers make up the platforms of an agent system.
- Hosts are the computing devices on which the infrastructure and agents execute, along with the hardware providing access to the world. This may range from common disk drives and displays to more specialized hardware such as GPS receivers or robotic effectors.
- Environment is the world in which the infrastructure and agents exist. This may include physical elements, such as the network connections between hosts, as well as computational elements, such as web pages the agents may access.

An agent system is simply a set of frameworks and agents that execute in them. A multi-agent system is an agent-based system that includes more than one agent. Such systems may consist of many agents running within a single framework instantiation, or in different frameworks, on different hosts, etc. In the agent system, the devices connected at the host layer via wireless networking, transmitting and receiving signals in the environment of the physical world.

3. Mobile Agent Security

Secure communication between agents is considered as a challenge because of the inherent complexity. In fact, security of agents can be viewed at different levels such as agent authentication, message authentication several works have been proposed to secure agent communication.[5]

Such systems decompose into several layers of hardware and software that provide an operating context for agents, situated computational process that sense and affect their environment. Note that the relationships across layers may be n-to-1.

With the advent of the extensive use of Intranets and the Internet, the possibilities of widespread use of distributed applications have come into focus. Mobile agent technologies offer developers the advantage of building applications that may be distributed across the network using high levels of abstraction. Although many advantages of mobile agents have been offered, the overriding advantage of their deployment is the ability to balance network and processing load among nodes in a network. Essentially, the mobile agent may be sent to the node where the resources with which it needs to deal are located. By so doing, local communication rates between the agent and its required resources increase, while overall

network traffic decreases. Mobile agents may also migrate to nodes that offer more processing resources for performing a task.[6]

For the wireless security especially the IEEE 802.11, the first five years of its life, IEEE 802.11 had only one method defined for security. This was called Wired Equivalent Privacy or WEP (often misidentified as Wireless Effective Privacy and other variants). In 2000, as Wi-Fi LANs increased in popularity, they attracted the attention of the cryptographic community, who rapidly detected cracks in the WEP approach. By the end of 2001, tools were available on the Internet designed to crack open WEP in a fairly short time. The IEEE 802.11 (1999) defined two levels of security: open and shared key. Open security really means no security. It is used in the same way that one would say, "I went to work and left the front door of my house open." Most people have figured out this is not a good security policy for their homes, and you probably feel the same way about Wi-Fi LANs. Shared key simply means that both ends of the wireless link know a key with a matching value. To be useful, this must be a secret shared only between trusted parties. The new subset is called Wi-Fi Protected Access (WPA). Many leading vendors have now produced software upgrades so existing product can be converted to support WPA and most new products are now shipped with WPA capability. The Wi-Fi Alliance has created a test plan for WPA so vendors can ensure interoperability.[7]

In terms of Security requirements, mobile agent environments are problematic. The push to use agent mobility entails having autonomous agents that can roam a network, from computer-to-computer based upon an itinerary generated by the agent, modulated by what the agent senses and its prescribed goals.

The purpose of security functionality is to prevent execution of undesirable actions by entities from either within or outside the agent system while at the same time allowing execution of desirable actions. The goal is for the system to be useful while remaining dependable in the face of malice, error or accident. Process Model: Security functionality is described by the following processes:[4]

- ***Authentication is*** a process for identifying the entity requesting an action.
- ***Authorization is a*** process for deciding whether the entity should be granted permission to perform the requested action.
- ***Enforcement is a*** process or mechanism for preventing the entity from executing the requested action if authorization is denied, or for enabling such execution if authorization is granted.

Some general technologies for achieving security include authorization models and mechanisms; auditing and intrusion detection; cryptographic algorithms, protocols, services, and infrastructure; recovery and survivable operation; risk analysis; assurance including cryptanalysis and formal methods; penetration technologies including viruses, Trojan horses, spoofing, sniffing, cracking, and covert channels.[4]

4. Advanced Encryption Standard (AES) Algorithm

In January 1997, the National Institute of Standards and Technology (NIST) invited proposals for new algorithms for the Advanced Encryption Standard (AES) to replace the old Data Encryption Standard (DES). After two rounds of evaluation on the 15 candidate algorithms, NIST selected the Rijndael as the AES algorithm in October 2000. [8]

The AES algorithm has broad applications, including smart cards and cellular phones, WWW servers and automated teller machines (ATMs), and digital video recorders. Compared to software implementations, hardware implementations of the AES algorithm provide more physical security as well as higher speed. Figure 2 shows the block diagram of AES algorithm.

The AES algorithm is a symmetric-key cipher, in which both the sender and the receiver use a single key for encryption and decryption. The data block length is fixed to be 128 bits, while the key length can be 128, 192, or 256 bits, respectively. In addition, the AES algorithm is an

iterative algorithm. Each iteration can be called a round, and the total number of rounds, Nr, is 10, 12, or 14, when the key length is 128, 192, or 256 bits, respectively. [8]
The 128-bit data block is divided into 16 bytes. These bytes are mapped to a 4x 4 array called the State, and all the internal operations of the AES algorithm are performed on the State.

5. The Lagrange Interpolation Polynomial

The problem of constructing a continuously defined function from given discrete data is unavoidable whenever one wishes to manipulate the data in a way that requires information not included explicitly in the data. The relatively easiest and in many applications often most desired approach to solve the problem is *interpolation*, where an approximating function is constructed in such a way as to agree perfectly with the usually unknown original function at the given measurement points. In the practical application of the finite calculus of the problem of interpolation is the following: given the values of the function for a finite set of arguments, to determine the value of the function for some intermediate argument. [9]

5.1 The Problem of Interpolation

The problem of interpolation consists in the following: Given the values y_i corresponding to x_i, i = 0, 1, 2, . . . , n, a function f(x) of the continuous variable x is to be determined which satisfies the equation:

$$y_i = f(x_i) \text{ for } i = 0, 1, 2 \ldots, n \quad \ldots..(1)$$

and finally f(x) corresponding to $x = x_0$ is required. (i.e. x_0 different from x_i, i = 1, n.)

In the absence of further knowledge as to the nature of the function this problem is, in the general case, indeterminate, since the values of the arguments other than those given can obviously assigned arbitrarily.
If, however, certain analytic properties of the function is given, it is often possible to assign limits to the error committed in calculating the function from values given for a limited set of arguments. For example, when the function is known to be representable by a polynomial of degree n, the value for any argument is completely determinate when the values for n + 1 distinct arguments are given. [9]

5.2 Lagrange Interpolation

Consider the function f : $[x_0, x_n] \rightarrow R$ given by the following table of values :

x_k	x_0	x_1	...	x_n
$f(x_k)$	$f(x_0)$	$f(x_1)$	...	$f(x_n)$

x_k are called *interpolation nodes*, and they are not necessary equally distanced from each other. We seek to find a polynomial P(x) of degree n that approximates the function f(x) in the interpolation nodes, i.e.:

$$f(x_k) = P(x_k); \; k = 0, 1, 2, \ldots, n.$$

The Lagrange interpolation method finds such a polynomial without solving the system. [9]

Theorem : Lagrange Interpolating Polynomial
The Lagrange interpolating polynomial *is the polynomial of degree* n *that passes through* (n + 1) *points* $y_0 = f(x_0)$, $y_1 = f(x_1)$, . . . $y_n = f(x_n)$. *let:*

$$P(x) = \sum_{j=0}^{n} P_j(x) \quad \ldots(2)$$

Where

$$P_j(x) = y_j \prod_{k=0, k \neq j}^{n} \frac{x - x_k}{x_j - x_k}. \quad \ldots.(3)$$

6. The Proposed System

The proposed system was designed to give solution for securing mobile Agent communication in wireless network. The proposed technique is depending on the encryption

techniques like AES 256bit algorithm. The proposed system will be used the Lagrange interpolation polynomial as encryption function used to encrypt the sending /receiving packets between Agent –server.

The proposed system (as shown in Figure 3) is built from two stages: first stage encrypts the data transport by using the Key generation (Lagrange interpolation polynomial key generation) and AES 128 bit algorithm.

In this stage, the Lagrange interpolation polynomial was used to generate the encryption key by using a pseudo key numbers. The encryption operation for this stage is by depending on the AES algorithm. The Lagrange key generation will he used in order to increase the strength of the key and to avoid the weak keys from using in the encryption operation. Figure 4 shows the key generation using Lagrange interpolation calculation.

The second stage is encrypting the resulted data from the first stage by the proposed Lagrange interpolation encryption operation key and XOR operation. In this stage, the encryption operation will do by using the Lagrange interpolation polynomial calculation to generate key (as shown in Figure 4) and will be used in the XOR encryption operation to encrypt the output stream from the AES algorithm (from previous stage). This stage was used to increase the randomness of the output data stream (in the packets) in order to get the benefits of the multi encryption techniques with less time of encryption as possible. Additionally, the encryption/decryption operations are designed to time efficient depending on the visual studio 2008 programming facilities.

The final encrypted data will send into the TCP/IP protocol services in order to encapsulate the outgoing/incoming packets to complete the communication between the Agents and master server computers through the local wireless network. In this proposed system, the local area wireless network was built from 10 computer connected using Ethernet wireless card of 54Mbps speed connection separated by average 1km

Note: in Figure 4, L_i is the Lagrange calculation output and K_{vi} is the element of (K_0 for first stage when v=0) or K_3 when v=3 in second stage of generation. K_j is generated encryption key (for j=1 in the first stage, and j=2 in the second stage of encryption). Also, the K_0 differs from K_2 to avoid the similarity.

The steps of the proposed system are:

In sending operation (For Agent program in the host computer connected to Agent server) case:

a. Loading the sending data.
b. Encrypt the sending data using (first the Lagrange interpolation polynomial key generation and AES algorithm with 128 bit key).
c. Encrypts the resulted encrypted data (from step b) using second Lagrange interpolation polynomial generation key and XOR encryption operation.
C. Establish the connection with the agent server.
d. Send the resulted encrypted data to TCP/IP protocol for sending the encrypted data to agent server.
e. Using one of the encryption wireless network technique like WAP, WEP and other.

In sending operation (For Agent server program in the server computer connected to Agent host) case:

a. Loading the sending data.
b. Encrypt the sending data using the first Lagrange interpolation polynomial key generation and AES algorithm with 128 bit key.
c. Encrypts the resulted encrypted data (from step b) using second Lagrange interpolation polynomial key generation with XOR encryption operation.
c. Establish the connection with the selected agent host.
d. Send the resulted encrypted data to TCP/IP protocol for sending the encrypted data to agent host.
e. Using one of the encryption wireless network technique like WAP, WEP and other.

In receiving operation (For Agent program in the host computer connected to Agent server) case:

a. Establish the connection with the agent server.
b. Loading the receiving packet from the TCP/IP protocol stack after decrypting packet using one of the encryption/decryption wireless network technique like WAP, WEP and other.
c. Decrypts the resulted data (from step b) using second Lagrange interpolation polynomial key generation with XOR encryption/decryption operation.
d. Decrypt the receiving data using the first Lagrange interpolation polynomial key generation and AES algorithm with 128 bit key.
e. Send the resulted data to Agent program to saving and displaying.

In receiving operation (For Agent server program in the server computer connected to Agent host) case:

a. Establish the connection with the agent server.
b. Loading the receiving packet from the TCP/IP protocol stack after decrypting packet using one of the encryption/decryption wireless network technique like WAP, WEP and other.
c. Decrypts the resulted data (from step b) using second Lagrange interpolation polynomial key generation with XOR encryption/decryption operation.
d. Decrypt the receiving data using the first Lagrange interpolation polynomial key generation and AES algorithm with 128 bit key.
e. Send the resulted data to Agent server program to saving and displaying.

Results and Conclusions

The proposed technique was applied to local wireless network of 1 router with 10 PC connected to this network (with up to 54MB bitrate). One of these computers works as a center server to agents. The others have the Agent connection program for many services of internet. The delays time was calculated in many services like navigation, downloading, uploading, and chatting in two cases (without and with applied proposed encryption technique). This local wireless network has a web server, FTP server, exchange server, and other services servers installed in the center agent server PC. The results were collected by testing local wireless network to 6 months with proper services and internet conditions. Good results were getting from applied the proposed algorithm, best and fast encryption message was transfered from the point to other points in wireless network.

From the results of applied the proposed algorithm (as shown in Table 1), the delay time was increased by 19s in minimum to -1.20 minutes from the original delay time (calculated for the same services without proposed algorithm). The QoS is calculating for this condition to this local wireless network and found approximately equals to 97% (QoS calculation depended on the number of received packet of the specific service to total packet sending through the network).

References

1. Shih, T. K. (2008),Cryptosystem Applications in Mobile Agent Security, Journal of Security Engineering, Article 5 (1), February.
2. Navarro, G. ; Ortega-Ruiz, J.A. ; Garcia, J. and Robles, S. (2003),Secure Agent-Based Management For Pervasive Environments, Spanish Government Commission CICYT, TIC2003-02041,.
3. Vladimirov, A. A. ; Gavrilenko, K. V. and Mikhailovsky,A. A. (2004),Wi-Foo - The Secrets Of Wireless Hacking “,Addison Wesley, June 28, , ISBN: 0-321-20217-1.

4. Mayk ,I. and Regli, W. C. (2006)Agent Systems Reference Model Release Version 1.0a ",DoD Contract #DAAB07-01-9-L504, -11-20 13:15:19 -0400.
5. Khemakhem, M. ; Rekik, W. and Fayolle, J. (2010),A flexible and secure web service architectural model based on PKI and agent technology", International Journal for Infonomics (IJI), Volume 3, Issue 2, June.
6. Korba, L. (1999), Towards Secure Agent Distribution and Communication", Proceedings of the 32nd Hawaii International Conference on Science Systems –0-7695-0001-3/99.
7. J. Edney, W. A. Arbaugh," Real 802.11 Security: Wi-Fi Protected Access and 802.11i", Addison Wesley, July 15, 2003, ISBN: 0-321-13620-9.
8. Zhang, X. and Parhi, K. K. (2004),High-Speed VLSI Architectures for the AES Algorithm", IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, 12, (9), SEPTEMBER.
9. Hussien,K. A. (2011),The Lagrange Interpolation Polynomial For Neural Network Learning", International Journal of Computer Science & Network Security ,11 (3) March.

Table (1): The Results Agent Connection After/Before Applied The Proposed System In Local Wireless Network

Service name	Size of data routing (MB)	Delay time in sending/receiving without proposed algorithm (average for MB)	Delay time with proposed algorithm (average for MB)
Navigation	8970	1s-1.30minutes	21s-1.54minutes
Downloading(HTTP)	38570	8s-4minutes	27s-2.90minutes
Downloading (FTP)	73400	15s-7minutes	50s-8.17min
Emailing	3200	5s-120s	30s-3.71minutes
Chatting	400	10s-120s	30s-200s

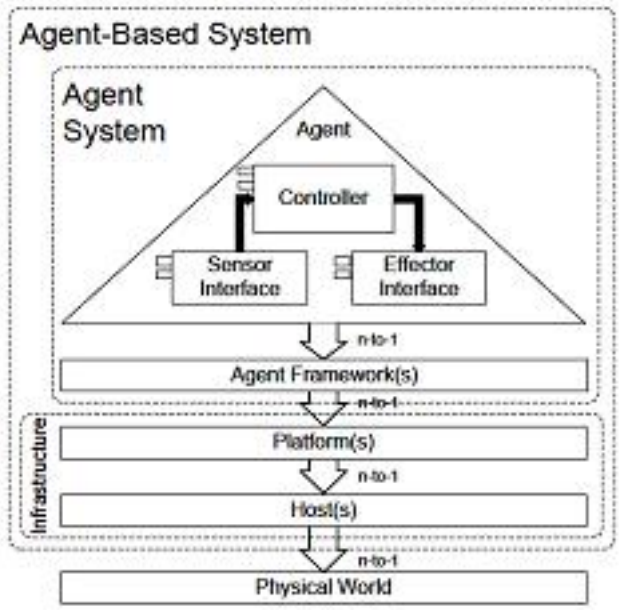

Fig. (1): Abstract model of an agent system.

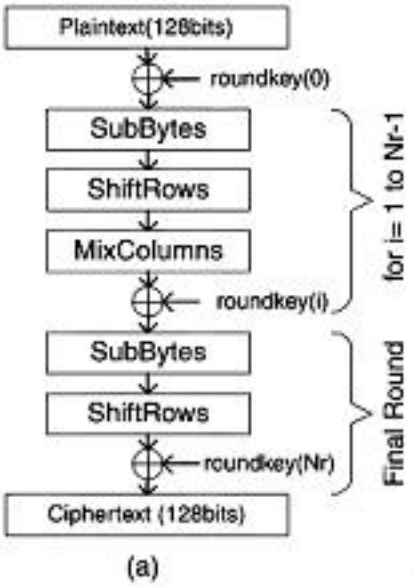

Fig.(2): The block diagram of the AES algorithm.

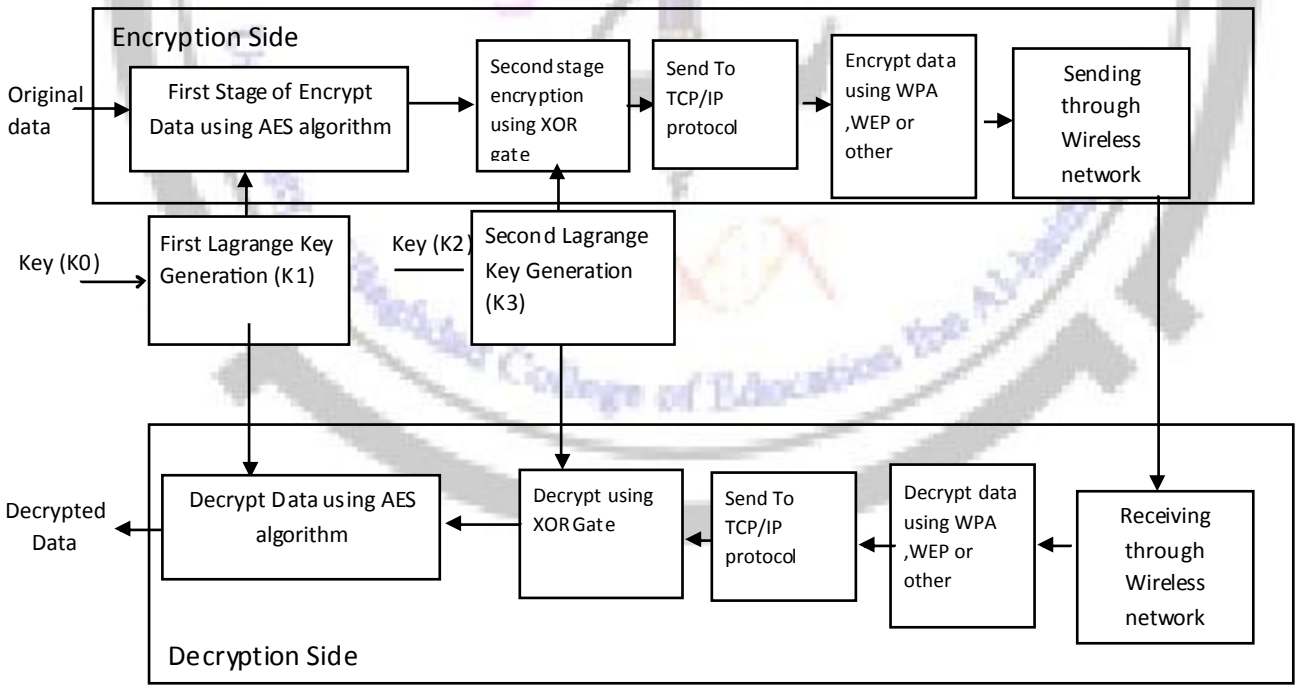

Fig.(3): The proposed Agent Connection Encryption/Decryption System

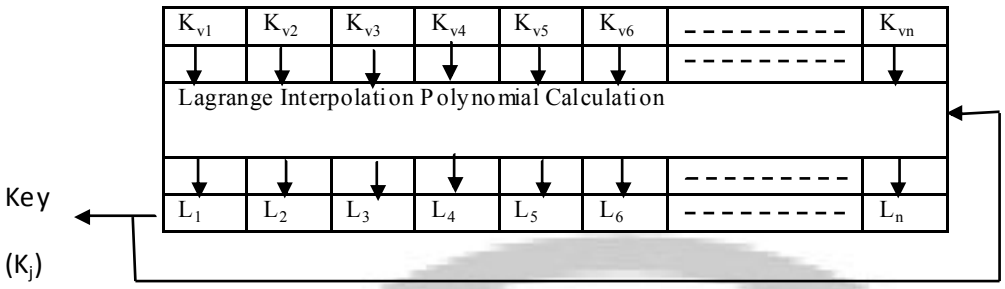

Fig. (4): The Lagrange Interpolation Polynomial Key Generation

Ibn Al-Haitham Journal for Pure and Applied Science
مجلة إبن الهيثم للعلوم الصرفة و التطبيقية
No. 1 Vol. 25 Year 2012
العدد 1 المجلد 25 السنة 2012

استيفاء لآكرانج لتشفير اتصال العميل المحمول

حيدر كاظم حمود
قسم علوم الحاسبات، كلية التربية، الجامعة المستنصرية

استلم البحث في : 6 حزيران 2011 ،قبل البحث في : 13 تموز 2011

الخلاصة

تقنية جديدة اقترحت من اجل اتصالات امينة مستعملة في نقل البيانات والتعليمات بين الوكيل والخادم في شبكة الاتصال اللاسلكية المحلية. يعتمد الأسلوب المقترح على مرحلتين من التشفير (استعمال خوارزمية AES ومتعدد استيفاء لاكرانج لتوليد مفتاح التشفير مدعومة ببوابة XOR) لتشفير الحزم. قد عدّل توليد مفتاح AES باستخدام مفاتيح المقترحة من تولد طريقة استيفاء لاكرانج لتفادي مفتاح تشفير ضعيف ثم نتائج جيدة للطريقة المقترحة من خلال إجراء عملية تشفير متعدد وفي وقت تشفير سريع وجودة عالية في عملية الاتصال.

الكلمات المفتاحية : Agent, Agent security, Mobile Agent, Lagrange interpolation application.

Ibn Al-Haitham Journal for Pure and Applied Science
مجلة إبن الهيثم للعلوم الصرفة و التطبيقية
No. 1 Vol. 25 Year 2012
العدد 1 المجلد 25 السنة 2012