

# A Mobile Agent Based Architecture for Securing WLANs

V. S. Shankar Sriram<sup>1</sup>, G. Sahoo<sup>2</sup>

<sup>1</sup>Birla Institute of Technology/Department of Information Technology, Ranchi, Jharkhand, India  
Email: sriram@bitmesra.ac.in

<sup>2</sup>Birla Institute of Technology/ Department of Information Technology, Ranchi, Jharkhand, India  
Email: drgsahoo@bitmesra.ac.in

**Abstract**—Wireless LANs are open and are vulnerable to various attacks. Techniques available to prevent Wireless LANs from these attacks are not comprehensive. In this paper we discuss the drawbacks of the existing security mechanisms and we provide a security architecture which uses Mobile agents as a security facilitator. Using this architecture, users have freedom to choose from a variety of encryption techniques presently available, to secure their Wireless LANs.

**Keywords**—Security, wireless LANs, mobile agent and encryption algorithm.

## I. INTRODUCTION

Much attention has been focused recently on the security aspects of existing Wi-Fi also called as (IEEE 802.11 a/b/g) Wireless LAN systems (WLANs). The 802.11a standard uses the same core protocol as the 802.11 legacy standard, operates in 5 GHz band width a maximum raw data rate of 54 Mbit/s, which yields realistic net achievable throughput in the mid-20 Mbit/s. The effective overall range of 802.11a is slightly less than that of 802.11b/g; 802.11a signals cannot penetrate as far as those for 802.11b because they are absorbed more readily by walls and other solid objects in their path. 802.11b has a maximum raw data rate of 11 Mbit/s and uses the same media access method defined in the original standard. 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard. The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology. The third modulation standard ratified was: 802.11g. This works in the 2.4 GHz band (like 802.11b) but operates at a maximum raw data rate of 54 Mbit/s, or about 19 Mbit/s net throughput. 802.11g hardware is fully backwards compatible with 802.11b hardware[7].

The rapid growth and deployment of these systems into a wide range of networks and for a wide variety of applications drives the need to support security solutions that meet the requirements of a wide variety of users. Wireless security can be broken into two parts, authentication and encryption. Authentication mechanisms can be used to identify a wireless client to an access point and vice-versa, while encryption Mechanisms ensure that it is not possible to intercept and

decode data. For many years, MAC access control lists have been used for authentication, and 802.11 WEP has been used for encryption. There are various other security mechanisms available for WLANs that include WPA and WPA2. But none of these seem to provide complete and comprehensive security.

In this paper we propose an architecture which uses mobile agents to achieve security in WLANs. Our architecture provides a secured means of key generation and key distribution which opens the avenue for the users of WLAN to choose an encryption technique of his choice. The target of this contribution is to evaluate current WLAN technologies with regards to security and present solutions to prevent wireless attacks. We implemented this architecture with java based Aglets<sup>™</sup> as mobile agents and Java Cryptographic Architecture (JCA) of JDK1.4<sup>™</sup> for cryptographic services. Using this, WLAN users need not limit themselves to WEP, WPA and WPA2 but can use any crypto algorithm supported by JCA.

## II. SECURITY THREATS IN WLANS

WLANs are vulnerable to various attacks of its openness. There are a variety of attacks possible over WLANs.[2] There are security mechanisms to counter act the attacks. In this section we discuss the most common attacks that are possible over WLANs.

### A. Eaves Dropping

Eavesdropping of network traffic is probably the biggest single threat affecting Wi-Fi networks. Passive listening of network traffic is virtually impossible to detect, and very little technical knowledge is required to perform it.[2] With right equipment it may be possible to listen traffic from few kilometers away. The only thing required to eavesdrop traffics to have a wireless network adapter in promiscuous mode and some kind of network analyzer software, which are publicly available on the Internet. The best protection against eavesdropping is to use a protocol that supports encryption. For users, this means a higher level protocol, such as SSL.

### B. Man in the Middle Attack

A man in the middle (MITM) attack is where someone funnels victim's traffic through a point controlled by the attacker[7]. This allows the attacker to view and modify every packet that goes through that certain point -

potentially every packet send by the victim. As wireless networks allows anyone within range to intercept Network traffic, has the risk of a man in the middle attack much higher than traditional wired networks.

### C. Denial of Service Attack

Denial of service attacks against wireless networks can be divided to three groups based on their target. First group of attacks target the transmission frequency used. Second group of attacks target the MAC layer of the Wi-Fi network, making it the most interesting layer regarding Wi-Fi networks. Last but not the least, attacks that target protocols on the higher levels, mainly TCP/IP or client/server systems directly.

## III. RELATED WORK

The security mechanisms for secure communications on 802.11 wireless networks have been developed in the following chronological order:

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- 802.11i (WPA2)

### A. Wired Equivalent Privacy(WEP)

WEP was the first methodology which was used to secure WLANs. The encryption used in WEP can be broken easily, even in practice [8]. There are various tools available on the Internet, which passively recover shared secrets used in WEP. Probably the most well-known tool is called AirSnort, available at <http://airsnort.shmoo.com>. The theoretical and practical weaknesses in WEP make it quite useless. It requires pre shared secrets, so it is not very flexible and therefore cannot generally be used corporate environments, nor in public hotspots

### B. Wi-Fi Protected Access (WPA)

WPA uses Temporal Key Integrity Protocol (TKIP) to improve WEP but also employs RC4 algorithm with modifications WPA uses 48-bit initialization vector for reducing probability of having similar keys, and Temporal Key Integrity Protocol for reducing replay attack, key management strategies, and MD5 to overcome collision flaws in the produced hashed value to provide stronger integrity level. [4]

### C. 802.11i (WPA2)

The long-term solution considered for wireless networks by Task Group i (TGi) is 802.11i, also called WPA2 . It is ratified as a standard in 2004. Although WPA is not vulnerable WPA2 solution has been designed by IEEE 802.11i because of possible flaws in WPA according to the WEP weaknesses.[1] 802.11i doesn't employ RC4 like WEP or WPA; it uses Counter Mode with CBC-MAC Protocol (CCMP) to encrypt network traffic.[3] CCMP employs Advanced Encryption Standard (AES) as encryption algorithm. 802.11i is backwards compatible with WPA but not with WEP.

Although AES based encryption is provided in WPA2, WLAN users do not have the flexibility to choose with other encryption algorithms like elliptic curve crypto algorithms and hyper elliptic curve crypto algorithms which prove to be better crypto mechanisms in terms of smaller key sizes and increased complexity from a crackers perspective.[6][7]

## IV. PROPOSED ARCHITECTURE

Our proposed architecture uses a Mobile agent server which is also the DHCP server used for allocating IP address. We used AGLET<sup>™</sup> as our mobile agent. The various components of the Mobile agent server are ASDK(Aglet software development kit) JDK1.4 (for utilizing java cryptographic Architecture) and the Java Runtime Environment(JRE). The architecture is shown in Figure 1.

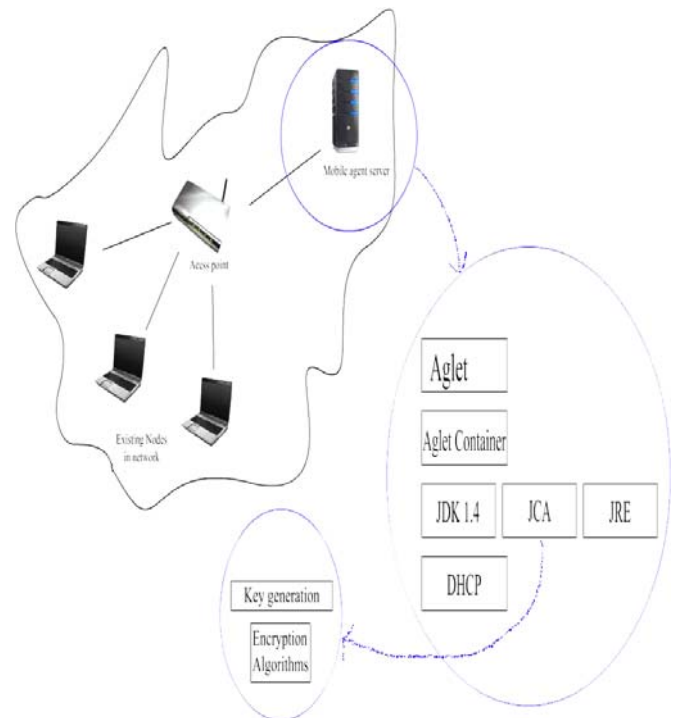


Figure 1. The proposed Architecture

The ASDK is a free download at [http://sourceforge.net/project/showfiles.php?group\\_id=7905](http://sourceforge.net/project/showfiles.php?group_id=7905) and can be used for development of Mobile agent based application. It has an AGLET<sup>™</sup> container called as the TAHITI environment, which takes care of the security of the mobile agent.

Java Cryptographic Architecture (JCA) provides with a variety of cryptographic services right from key generation process (using the sand box) to a variety of encryption algorithms where from users can easily choose the algorithm of his choice.

We propose a Key generation algorithm and a Key distribution mechanism to make this architecture efficient. The Key generation process consists of 3 steps. Generation of  $MCN_i$  (Key generated with respect to individual nodes), Generation of  $MCS_i$  (Key generated

with respect to the access point) and generation of  $K_i$ , the final key which is unique between the wireless node and the access point. Between the access point and every individual node there exists  $K_i$ , which is unique. The key distribution is facilitated through the mobile agents. The key generation process and the algorithm which specifies the entire operation are as follows.

**A. Key Generation Mechanism**

In this section, we propose a key generation mechanism which is carried out in three steps. This technique to generate the key is robust and the key is shared between the slave agent and the master agent to secure the communication channel between Node and Server. The MAC address, IP address and the Host name are got from the DHCP server. As soon as a wireless client comes into the vicinity of the access point the first operation is to issue an IP address. In this process the DHCP server gathers the MAC address. The MAC address, IP address and the Host Name are used in the key generation process. The internal mechanism to generate the key is defined below and the algorithm that supports this encryption technique is defined in the next section.

**Step 1: Generation of  $MCN_i$**

To generate the Mix Column ( $MCN_i$ ) for Node  $N_i$

1. Append the Name (48 bit), Mac address (48) and IP address (32) of node  $N_i$  to get a 128 bit of length Bit Sequence of the node ( $BN_i$ ).
2. Generate a Random number ( $R_i$ ) of 128 bit length Mix columns of both  $BN_i$  and  $R_i$  and the final  $MCN_i$  is Generated as shown in Figure 2

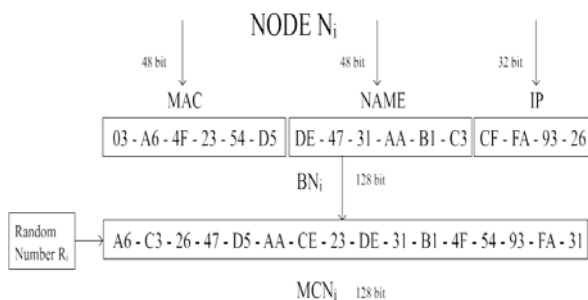


Figure 2. Generation of  $MCN_i$

**Step2: Generation of  $MCS_i$**

To generate the Mix Column ( $MCS_i$ ) for Server S

1. Append the Name (48 bit), Mac address (48) and IP address (32) of Server S to get a 128 bit of length Bit Sequence ( $BS_i$ ).
2. Generate a Random number ( $R_i$ ) of 128 bit length
3. Now Mix columns of both  $BS_i$  and  $R_i$  and the final  $MCS_i$  is generated as shown in Figure 3.

**Step 3: Generation of final key  $K_i$**

To generate the final key

1. Perform Mask operation on both  $MCS_i$  and  $MCN_i$ , consider the output as Partial Key (PK).



2. Now perform S BOX operation on PK and Key Length ( $L_i$ ) which is generated by Encryption

Figure 3. Generation of  $MCS_i$

3. Algorithm performed on Node  $N_i$  and the final key ( $K_i$ ) is generated as shown in Fig. 4

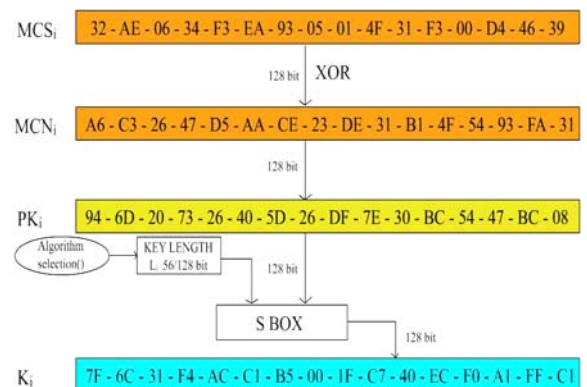


Figure 4. Final Key Generation

**B. Algorithm supporting the proposed mechanism**

/\* Notational explanation\*/

IP-IP address, MAC- MAC Address, NAME-Name of the node as in the DHCP, NODE-Wireless client.

/\* Algorithm for Checking the Presence of A Valid Node \*/

1. A node  $N_i$  enters the vicinity of Access-point S.
2. After  $N_i$  entering into vicinity, S checks for open port  $P_i$  (port no.: 4434).  
If  $P_i$  exists  
Go to Step 3.

Else

Discard node  $N_i$ .

/\* Algorithm to Select an Encryption Algorithm \*/

3.  $\forall A \in$  Encryption algorithms supported by JCA, choose an algorithm  $A_i$ .

Function\_keylength (Algorithm  $A_i$ )

Return key length  $L_i$ .

/\* Algorithm to Generate the Key \*/

4. Acquire node  $N_i$ 's IP, MAC and NAME from the server S.

If length of NAME = 48

Go to step 5.

Else if length of NAME <48

Pad '\*' until length = 48.

Go to step 5.

Else if length >48

Discard the bits  $B_j$ :  $j > 48$  and  $B_j \in$  NAME  $\forall j$ .

Go to step 5.

5. Append NAME, MAC and IP of node  $N_i$  to generate 128-bit sequence  $BN_i$ .
6. Acquire IP, MAC and NAME of access-point S.
  - If length of NAME = 48  
Go to step 7.
  - Else if length of NAME <48  
Pad '\*' until length = 48.  
Go to step 7.
  - Else if length >48  
Discard the bits  $B_j$   
 $j > 48$  and  $B_j \in \text{NAME} \forall j$ .  
Go to step 7.
7. Append NAME, MAC and IP of access-point S to generate 128-bit sequence BS.
8. Generate a random number  $R_i$ .
9. /\* Mix column using function MC \*/
  - Input\_MC ( $R_i, BN_i$ )
  - Return ( $MCN_i$ ).
  - Input\_MC ( $R_i, BS_i$ )
  - Return ( $MCS_i$ ).
- $\forall i$ : lengthof ( $BN_i, MCN_i, BS, MCS_i$ ) == 128 bit.
10. /\* Perform MASK operation \*/
  - Partial key  $PK_i = (MCN_i) \text{ XOR } (MCS_i)$ .
11. /\* S-box operation \*/
  - S-box ( $L_i, PK_i$ )
  - Return Key  $K_i$ .
  - $\forall i$  length of  $K_i = L_i$ .
12. /\* In master \*/
  - Master\_class (Key  $K_i$ )
  - Return Slave ( $K_i$ ).

C. Key Distribution using Mobile Agents

Key distribution in a Wireless environment is a critical issue because of its openness. The key distribution process can be made secured using mobile agents. Before handing over the key to the appropriate node, the agent checks for the node's authenticity. The Master Agent running at the Mobile agent server takes care of this by dispatching a slave agent to every node that is associated to the access point. A slave agent carries the key along with the code for checking the node's authenticity. Upon reaching the node the slave agent starts executing the code which checks the node's authenticity. The authentication process is based on MAC address of the node available with the Mobile agent server. If the MAC address posed by the node to the mobile agent server and the actual MAC address of the node match, the slave agent delivers the key. If there is a mismatch the slave agent informs the Master agent running in the Mobile agent server which results in the termination of the connection.

V. EXPERIMENTAL RESULTS

The explained architecture was implemented and found that our agent based architecture can be put into use for securing WLANs. Mobile agents react dynamically and autonomously to the changes in their

environment, which makes them robust, and fault tolerant. They have the ability to distribute themselves in the network in such a way as to maintain the optimal configuration for solving the particular problem. These characteristics make mobile agents the right technology to be used as a facilitator for enhancing security in Wireless LANs. The AGLET™ worked fine in the Wireless environment with AES (Advanced Encryption standards) based encryption. This can be extended to all the cryptographic algorithms supported by JCA. The starting of the AGLET and the login is shown in Figure 5. The screen shot of communication with AES based encryption between the master and slave agent is shown in Figure 6(a) & 6(b).

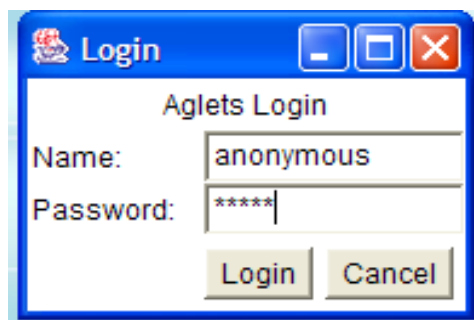
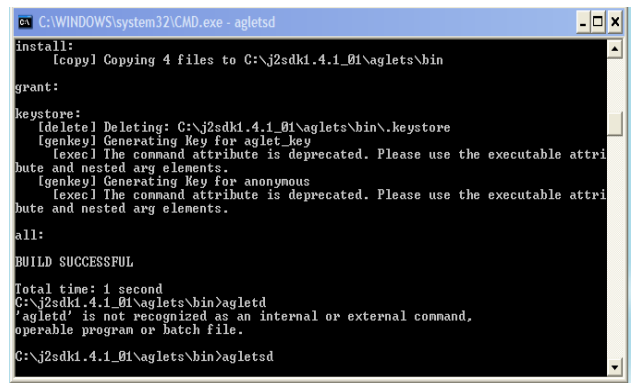


Figure 5. Aglet Started & Login Action

Using this architecture, users have the flexibility to choose with other encryption algorithms supported by JCA, like elliptic curve crypto algorithms which prove to be better crypto mechanisms than traditional cryptosystem with high speed, low computation time and resource consumption, which are well suited for wireless environments.

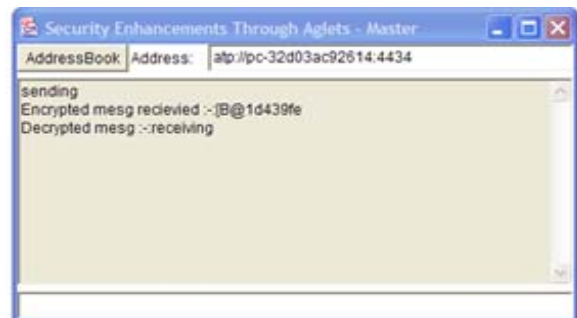


Figure 6(a). Master Aglets in Action

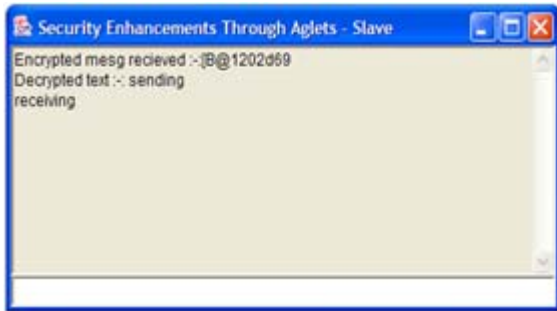


Figure 6(b). Slave Aglets in Action

#### CONCLUSION AND FUTURE WORK

The aglet based solution offers both security and enhanced performance in terms of speed at no cost. Moreover Aglets is a java based mobile agent and is inter-operable with java platform, hence can be easily integrated into the customer's software. Using a MAC, IP based security in a wireless environment with a DHCP backbone enhances the security in organizations where security is the main concern. So, enhancing 802.11 standards with the mobile agents may yield fruitful results. Our proposed algorithm for key generation generates a 128 bit key and can be extended according to the algorithm to be used. However, in spite of significant development in the field of cryptography there still exist many security issues that need to be addressed in mobile agents and will consider it as future work.

#### REFERENCES

- [1] Jyh-cheng chen, ming-chia jiang, and yi-wen liu "wireless lan security and IEEE 802.11i" IEEE Wireless Communications February 2005.
- [2] Franjo Majstor, "WLAN Security Threats & Solutions", Proceedings of the 28th Annual IEEE International Conference on Local Computer Networks (LCN'03)
- [3] Phillip Rogaway, "OCB Mode: Parallelizable Authentication Encryption" Preliminary Draft: October 16, 2000.
- [4] Wi-Fi Alliance. Wi-Fi protected access: Strong, standards-based, Interoperable security for today's Wi-Fi networks. April 2003.
- [5] Mohammad Abdul Azim and Abbas Jamalipour, "An Efficient Elliptic Curve Cryptography based Autheticated Key Agreement Protocol for Wireless LAN Security", School of Electrical and Information.
- [6] "Elliptic Curve Cryptography", Standards for efficient Cryptography Group, <http://www.secg.org>.
- [7] [en.wikipedia.org/wiki/IEEE\\_802.11i](http://en.wikipedia.org/wiki/IEEE_802.11i).
- [8] Mantin s. Fluher and a. Shamir. Weaknesses in the Key scheduling algorithm of rc4. 2001.
- [9] Wang Shunman, TaoRan, WangYue, ZhangJi, "WLAN and It's Security Problems", BeiJing Institute of Technology, BeiJing,P.R.China, 100081.