Int. J. Communications, Network and System Sciences, **2013, 6, 443-450**
http://dx.doi.org/10.4236/ijcns.2013.610046 Published Online October 2013 (http://www.scirp.org/journal/ijcns)

Wireless Network Security: The Mobile Agent Approach

Olatunde Abiona[1], Adeniran Oluwaranti[2], Ayodeji Oluwatope[2], Surura Bello[2], Clement Onime[3], Mistura Sanni[2], Lawrence Kehinde[4]

[1]Department of Computer Information Systems, Indiana University Northwest, Garry, USA
[2]Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria
[3]Information and Communication Technology Section, Abdus Salam International Centre for Theoretical Physics, Trieste, Italy
[4]Department of Electrical and Electronic Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria
Email: oabiona@iun.edu, aranti@oauife.edu.ng, aoluwato@oauife.edu.ng, apinkebello@yahoo.com, onime@ictp.it, misturasanni@gmail.com, lokehinde@oauife.edu.ng

Received August 12, 2013; revised September 14, 2013; accepted September 21, 2013

ABSTRACT

The broadcast nature of wireless network makes traditional link-layer attacks readily available to anyone within the range of the network. User authentication is best safeguard against the risk of unauthorized access to the wireless networks. The present 802.1× authentication scheme has some flaws, making mutual authentication impossible and open to man-in-the-middle attacks. These characteristics make traditional cryptographic mechanism provide weak security for the wireless environment. We have proposed the use of mobile agents to provide dependable Internet services delivery to users, this will guarantee secure authentication in wireless networks and we examine the feasibility of our solution and propose a model for wireless network security.

Keywords: Wireless Network Security; Mobile Agent; Authentication

1. Introduction

Wireless networks has been experiencing an explosive growth similar to the Internet, this is due largely to the attractive flexibility enjoyed by both users and service provider. Some of the benefits are: network coverage without the cost of deploying and maintaining wires, mobility support and roaming which grant the users "anytime", anywhere access to network. While the emergence of these new technologies can enable truly ubiquitous Internet access, it also raises issues with the dependability of the Internet service delivered to users. Basically Wireless Local Area Network (WLAN) can operate in two modes, the infrastructure based and the ad hoc networks. Many organizations are deploying the infrastructure based wireless network to provide connectivity to places difficult to reach by cabling, to complement the existing wired networks. A lot of attention has been given to the provision of these wireless network solutions, but little attention has been given to the provision of adequate security for the emerging wireless networks making these networks prone to traditional link-layer attacks readily available to anyone within the range of the wireless network.

Wireless network security is more concentrated and complex than security of wired networks because wireless is broadcast in nature, making it possible for anyone within the range of a wireless device to intercept the packets sent without interrupting the flow of data between the wireless device and the access point. User authentication is the best safeguard against the risk of unauthorized access to the wireless network. The security features for mobile communication system include: confidentiality on the air interface, anonymity of the user and, most importantly, authentication of the user to the system in order to prevent fraudulent use of the system [1]. Wireless network security is different from wired network security primarily because it gives potential attackers easy transport medium access. This access significantly increases the threat that any security architecture must address. Unfortunately, the early IEEE 802.11 standards failed to account for it [2]. Hence the security schemes in wired network can not be used directly in wireless network.

A typical wireless infrastructure network consists of a wireless device known as a stations (STAs) communicating with a centralized stationary Access Point (AP)

over a wireless channel. Security threats against the wired network are equally applicable to the wireless networks, but the wireless networks suffer a number of additional vulnerabilities that make it more challenging to secure [3].

- Open wireless medium: The security threats of message eavesdropping and injection are universal in any network; however, they are more severe in wireless networks due to open wireless medium.
- Limited bandwidth: Wireless networks are particularly vulnerable to denial-of-service (DoS) attacks and in-band signaling.
- System Complexity: Wireless networks are far more complex than the wired networks due to the special needs for mobility support and efficient channel utilization.

Mobile Agent (MA) is an effective paradigm for distributed applications and is particularly attractive in a dynamic network environment involving partially connected computing elements. MA is defined as a software component which is either a thread or a code carrying its execution state to perform the network function or an application [4]. MA can act as a middleware and perform network and other application related functions based on the underlying infrastructure: fixed wired networks, wireless cellular network or mobile ad hoc network [4]. MA paradigm is an emerging technology for developing applications in open, distributed and heterogeneous environment like the Internet. Agents have the ability to decide autonomously where to migrate to after they are dispatched. MA technology offers several advantages in many application areas, such as e-commerce, mobile computing, network management and information retrieval [4]. MAs are designed to execute locally on data at their destination, thus reducing network traffic and latency. Furthermore, MA asynchronous interaction can provide efficient solution in the case of unreliable and low bandwidth connection, to support mobile users that could disconnect while their agent still roam in the network. However, security is a major technical obstacle to wider acceptance and is of fundamental concern for mobile agent based system [4]. We explore the possibilities of using MAs for the provisioning of dependable Internet services delivery that meets the user's requirement in terms of security, by providing secure authentication in wireless networks.

The rest of the paper is organized as follows: Section 2 presents security challenges in wireless network. Section 3 presents wireless network security approaches. In Section 4, mobile agents and wireless network were discussed. In Section 5, mobile agents and security were discussed. In Section 6, mobile agent authentication scheme was discussed and the paper finally concluded in Section 7.

2. Security Challenges in Wireless Networks

Securing wireless networks posses unique challenges compared to a wired network due to the open nature of the access medium. In general, wireless networks suffer from security threats of wired networks and additional vulnerabilities making it more challenging to secure. Wireless network security is different from wired network security primarily because it gives potential attackers easy transport medium access. Hence the security schemes in wired network can not be used directly in wireless network. The fact that data are being broadcast via radio waves rather than transmitted over a wire introduces security challenges namely:

- How can you prevent user credentials from being hijacked during authentication negotiation?
- Once authentication is complete, how can you protect the privacy of the data being transmitted between client and access point? And finally,
- How can you make sure the authorized user connects to the right network?

The concerns are that of authentication, data confidentiality and privacy, data integrity, availability and rogue access point.

Authentication-Most password-based protocols in use today rely on a hash of the password with a random challenge. The server issues a challenge, the client hashes that challenge with the password and forwards a response to the server, and the server validates that response against the user's password retrieved from its database. Legacy password protocols are easily subjected to eavesdropping and man-in-the-middle attacks. An eavesdropping attacker can easily mount a dictionary attack against such password protocols. A man-in-the-middle attacker can pass through the entire authentication, and then hijack the connection and act as the user.

Data Privacy-Another concern is the security of the wireless data connection between the client and access point subsequent to authentication. While client and access point could easily negotiate keys subsequent to authentication, if the keys are not cryptographically related prior to the authentication, the data session would be subject to a man-in-the-middle attack. Therefore it is incumbent upon the authentication negotiation to result in keys that may be distributed to both client and access point to allow the subsequent data connection to be encrypted.

Rogue Access Point-A final security challenge results from the possibility that someone could install a WLAN access point and network and fool your user into doing work on that network. Rogue access points are those installed by users without coordinating with IT unit. Because access points are inexpensive and easy to install, rogue installations are becoming more common.

Limited Bandwidth—The networks that connect handheld wireless devices such as phones and Personal Digital Assistants (PDAs) suffer from low bandwidth and high incidence of network errors. Mobility can also result in the loss or degradation of wireless connections [5]. Limited communication bandwidth may also be a target for malicious attacks such as DoS attack. To implement such attack, the malicious node may send vicious queries flooding to target nodes to consume the bandwidth and occupy the shared wireless media, making the network services unavailable to other nodes [4]. Apart from the limitation in bandwidth constraint, each node in a wireless communication and mobile computing has limited transmission range and limited power supply.

System Complexity-Wireless networks are far more complex than the wired networks due to the special needs for mobility support and efficient channel utilization. It should be noted that each complexity in the system, adds additional security vulnerability to the wireless networks especially for systems with large user population and complex infrastructure [3].

3. Wireless Network Security Approaches

The Wireless Equivalent Privacy (WEP) protocol [3] was the first link-layer security mechanism introduced in 802.11 to provide a security level compared to that of with a physical wire. Unfortunately it is also fairly insecure. Hackers can easily find out the password and then do anything they want with your network. The software for doing this is widely available. Unfortunately, several security flaws in WEP were soon identified, which can be exploited to defeat its security goals [6].

The Wi-Fi alliance, a non-profit international association formed in 1999 to certify interoperability of WLANs, developed the Wi-Fi protected access (WPA) to enhance security level [7]. WPA addressed most of the security threats not resolved by WEP. WPA applies stronger network access control, supports better security technology, and enforces data integrity. However, WPA has some security flaws similar to WEP which poses additional threat and concerns namely:

- Encryption weakness—WPA suffer from encryption weakness making it possible for data tampering and masquerading attacks.
- Poor performance—Due to intensive computation of authentication and encryption, data transfer and communication speeds drops.

The IEEE 802.11i provides the highest level of security for the wireless networks by eliminating most of the security flaws in WEP and WPA and providing 128bit encryption security for wireless networks. However there is deterioration in performance as the network runs scripts to perform security checks and encryption. The major difference between WPA and IEEE 802.11i (also known as WPA2) is that WPA uses the temporal key integrity for confidentiality and MICHAEL for data integrity [3]. One major concern in the design of Michael is to reduce the computation overhead which resulted in its weak defense against message forgery. The IEEE 802.11i wireless security standards consist of three major components namely:

- Temporal Key Integrity (TKIP)
- Counter mode Cipher Block Chaining with Message Authentication Code (counter mode CBC-MAC) and
- 802.1× port based authentication for wireless client access control.

The IEEE 802.1× employs the Extensible Authentication Protocol EAP [8] over Local Area Network (LAN) called the EAPoL. The EAP is a transport framework that runs over link layer protocol and also has support for multiple authentication mechanism. The EAP framework is based on request and response. The IEEE 802.1× has three majorcomponents namely:

- Supplicant–client card,
- Authenticator–access point and
- Authentication server.

The supplicant is a station wishing to have access to the network, an authenticator, acting as a bridge between the supplicant and the authentication server. The Remote Authentication Dial in Service (RADIUS) protocol contains mechanism for per packet authenticity and integrity verification between AP and the RADIUS server [8]. EAP authentication begins with the authenticator sending an identity request to the supplicant. The identity response provided by the supplicant is sent from the authenticator to the authentication server. The authentication server determines the success or failure of the supplicant's request for authentication. Although the use of 802.1× is recommended for authentication, neither WPA nor WPA2 provided mutual authentication. Secondly the EAP is susceptible to Man-in-the-middle attack, since an attacker could forge success message from authenticator to supplicant [8]. The use of MA technology could provide a solution for mutual authentication and man-in-the-middle attack through the use of certificates and encryption of the MA.

4. Mobile Agents and Wireless Network

The concept of MA is different from Remote Procedure Calling (RPC), in that the RPC paradigm views computer-to-computer communication as enabling one computer to call procedures in another computer across the network [9]. Each message that the network transport either request or acknowledge a procedure's performance. E.g. a request includes data that are the procedure's argument, consequently the response include data that are

its results. **Figure 1** shows the RPC concept.

An alternative to remote procedure calling is Remote Programming (RP). The RP paradigm views computer-to-computer communication as enabling one computer not only to call procedures in another computer, but also to supply the procedure to be performed [9]. The only message that the network transport is composed of, a procedure that the receiving computer is to perform and the data that are its arguments. Such procedure calls are local rather than remote. The procedure and the state are termed a mobile agent. **Figure 2** shows the Remote Programming paradigm.

The advantage of remote programming is that a user computer and a server can interact without using the network once the network has transported an agent between them. Thus ongoing interaction does not require ongoing communication, leading to improved performance and better customization of functionality. MAs are programs that can migrate from one host to another in a network or at times to any host of their choice making them autonomous.

Wireless networks are characterized by the ability of the client or station to move freely at will, this movement has impact on the security of the network. The security implementation based on trust is confronted with great challenges and the static security mechanisms are not applicable in a dynamic environment. The mobility of clients may cause frequent breaks in the link resulting in data loss since the station can join and leave the network without prior notice. This implies that the connections between the client and the server may not be guaranteed at all times in the communication. This intermittent transmission has great impact on the information communication in wireless networks which may affect applications and security implementation. The mobile nodes in a wireless network could range from laptops, PDA to cellular phones. These devices are battery powered and the battery life time becomes crucial for wireless communication and mobile computing. Wireless networks also suffer from limited communication bandwidth; this may be a target for malicious attacks such as DoS attacks.

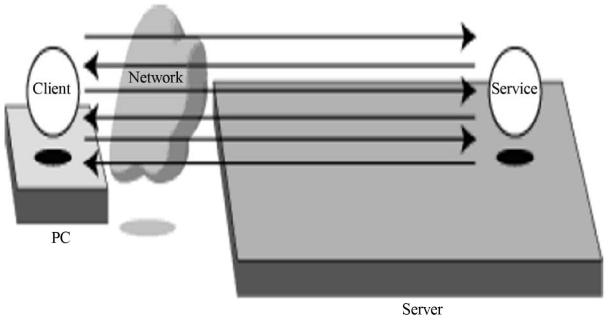

Figure 1. Remote procedure calling paradigm.

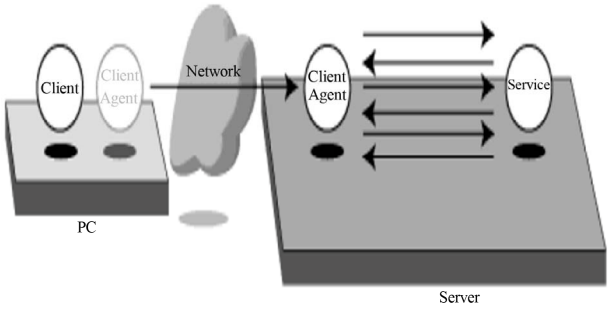

Figure 2. Remote programming or mobile agent paradigm.

Several benefits and advantages of using mobile code and mobile agent computing paradigms have been outlined in [10]. These include:

- Overcoming network latency
- Reduced network load
- Asynchronous and autonomous execution
- Adapting dynamically
- Encapsulating protocols
- Operation in heterogeneous environment
- Secure brokering
- Robust and fault-tolerant
- Well suited for e-commerce
- Can operate as personal assistant
- Distributed information retrieval
- Telecommunication network services
- Monitoring and notification
- Information dissemination and
- Parallel processing.

Considering the many advantages offered by MA, a major technical obstacle to a wider acceptance of the MA paradigm is security. Both agents and execution environments are prone to unwanted attacks and require appropriate protection mechanism. Some efforts at improving MA security include: Java sandboxes, type safe languages, software fault isolation and secure and open mobile agent (SOMA) [11].

By employing mobile agents, such mobile devices could provide a reliable technology for message transport over the wireless link. MAs are inherently distributed software entities that reduce the load on the network when they move. In addition they support disconnected operations since they continue to execute after they move, even if they lose network connectivity with their dispatcher [5]. MAs can be employed in wireless mobile devices in two ways: An agent platform could be installed on the devices, enabling MAs to run directly on them, or mobile devices could access and use remote MAs running on a wired network.

5. Mobile Agents and Security

MA security can be considered using a simple model

consisting of an agent and the agent platform. An agent is comprised of the code and the state information for carrying out some computation, mobility enables the agent to move among agent platform and the agent platform provides the computational environment for the agent to operate. The platform from which the agent was dispatched is known as the home platform, this is the most trusted environment for an agent. An agent system model is shown in **Figure 3**. One or more hosts may comprise an agent platform, and an agent platform may support multiple computational environments or meeting places, where agents can interact.

Mobile agents moving around the network are not safe. There are four known threat MA, namely: The Agent-to-Host, Agent-to-Agent, Host-to-Agent, Other-to-Agent Host attacks are the kinds of security attacks that are possible in a Mobile Agent System [12].

5.1. Protecting the Agent Platform

A major concern with agent system implementation is to ensure that agents are not able to interfere with one another or with the agent platform. Some techniques used for protecting agent platforms are described in detail in [12]. This includes:

- Software-based fault isolation (sandboxes)
- Safe code interpretation
- Signed code
- State appraisal
- Path Histories and
- Proof Carrying code

Another technique proposed in [13] replaced the Trusted Processing Environment (TPE) by a software machine called Secure Virtual Machine (SVM). The SVM is a software layer installed between the operating system and the agent environments. The platforms to be visited by the agent must have a certified SVM. On a platform, SVM receive an agent and creates an instance of SVM to execute only this agent in an allocated memory space called closed environment. Finally, before migration, the agent will be associated with a signed stamp that contains the actual platform time and the next platform time.

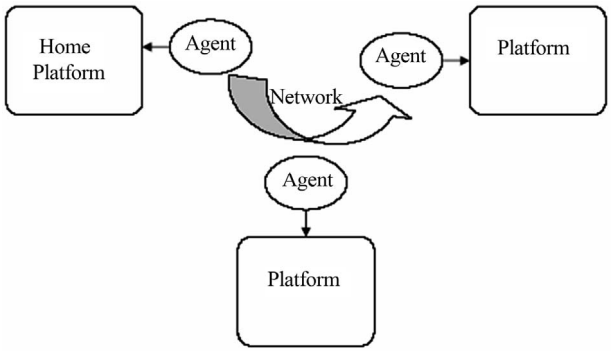

Figure 3. Agent system model.

5.2. Protecting Agents

While countermeasures directed towards platform protection emphasizes active preventive measures, countermeasures directed towards agent protection tend towards detection measures as a deterrent. Once an agent arrives at a platform, little can be done to stop the platform from treating the agent in any manner. The problem is usually referred to as the malicious platform problem. Some techniques used for protecting agents are described in detail in [12]. This includes:

- Contractual agreements
- Trusted hardware
- Trusted nodes
- Mutual itinerary recording
- Execution Tracing
- Environment key generation
- Co-operating agents
- Encrypted payload
- Computing with encrypted functions
- Undetachable signatures
- Obfuscated code

So far, there are no known techniques for an attacker to reverse engineer an agent's code.

6. Mobile Agent Athentication Scheme

The provisioning of dependable Internet service delivery that meets the user's requirement in terms of security requires strong access control. In order to protect the wireless networks from parking lot attackers, strong access control ideally on per packet basis must be enforced. Furthermore, mutual authentication should also be performed, since access points are untrusted entities from the supplicant's point of view. User authentication is best safeguard against the risk of unauthorized access to the wireless networks. However, one emerging technology could be much more adaptive than others in such environment. This technology is the mobile agent. We explore the feasibility of the Mobile Agent approach in our solution to the security problem inherent in IEEE 802.1× authentication and key management.

The MA paradigm is an emerging technology for developing applications in an open, distributed and heterogeneous environment. MAs are programs that can migrate from host to host in a network, sometimes they migrate to places of their choice. The state of the running program is saved, transported to the new host, restored, and execution continues from where it left off. Agents are software which represents the behavior of the users in the world of computer network. Some MA characteristics are as follows [14]:

- Reactive
- Autonomous
- Object-oriented
- Mobile
- Learning
- Believable

Some examples of mobile agents are; Aglets, Voyager, Odyssey, Concordia, ARA, Mole, Agent TCL, TA-COMA and SHIP-MAI. The four commonly used application environment for MAs are Aglets, Voyager, Odyssey, and Concordia [14].

MAs are small in size, they do not constitute a complete application by themselves, but rather they form an application by working in conjunction with an agent platform and other agents. Areas of concern in wireless network security include:

- Authentication
- Integrity and
- Confidentiality

Our focus is on authentication in wireless infrastructure network and we explore the feasibility of mobile agents as a solution to the inherent security problem of IEEE 802.1× authentication and key management. The following describe in detail Mobile Agent Wireless Authentication Architecture (MAWAA).

6.1. Security Model for the Scheme

The proposed security model is based on the IEEE 802.1× authentication protocol setup, involving the following three components [15]:

- Supplicant
- Authenticator and
- Authentication server.

Below we describe some of the abbreviations used in this paper. The security framework comprises of the following:

- Supplicant Platform
- Supplicant Mobile Agent (SMA)
- Supplicant Mobile Agent with Certificate (SMA Cert)
- Authenticator (Access Point)
- Authentication Server Platform
- Authentication Server Static Agent with certificate (ASSA Cert)
- Mobile Agent Wireless Authentication Architecture (MAWAA)

The mobile agent interaction model is shown in **Figure 4**. This model shows client/server communication and mobile agent communication. The mobile agent represent the client, carrying authentication details of the client and using this detail to authenticate the client to the server by exchanging request and response with the server. **Figure 5** shows a generic mobile agent framework, with agent manager, event manager, security manager and persistent manager.

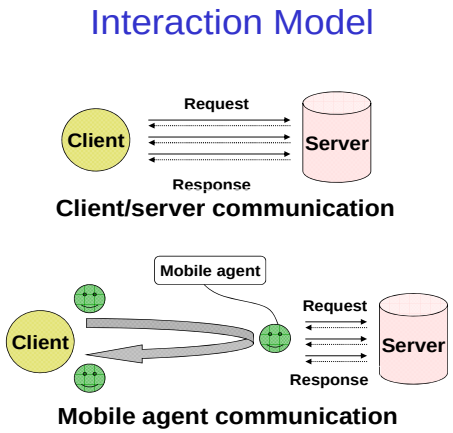

Figure 4. Interaction model.

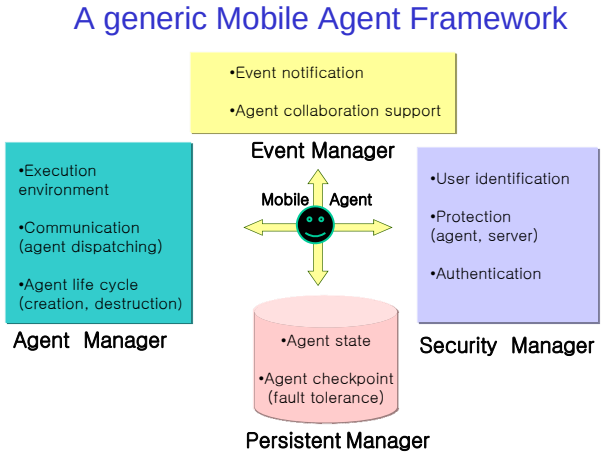

Figure 5. Generic mobile agent framework.

The proposed mobile agent wireless authentication Architecture is shown in **Figure 6**. Agent platforms are installed on both the supplicant and the authentication server; this will enable MA to run directly on them. When a supplicant come within the range of an authenticator, the authenticator sends a request for identification of the supplicant, the supplicant will then dispatch the SMA carrying all the required authentication information for the supplicant *i.e.* username, password and platform details for that particular user to the authentication server platform.

The Authentication Server Static Agent (ASSA) Cert is a static agent residing on the authentication server platform; the ASSA Cert combines two functions:

- Certificate Authority—in charge of the issuing and the management of certificates
- Authentication server—for authenticating users, agent, and platforms.

The Suplicant Mobile Agent (SMA) will meet with the ASSA Cert for the authentication process. A mutual authentication between SMA and ASSA Cert is carried out. If the authentication process is successful, then the net-

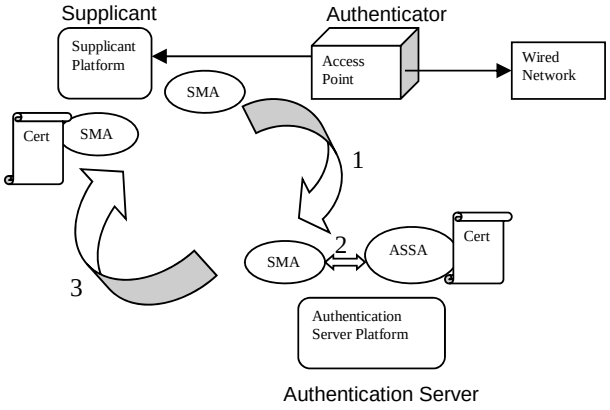

Figure 6. MAWAA authentication model.

work port on the authenticator closes and the supplicant will now have access to the network. The SMA will now be issued a certificate to become SMA Cert before returning to the supplicant platform.

6.2. Re-Authentication and Roaming MA

In order to increase security, re-authentication of users is done in some interval of time during the connection; this will ensure that a user cannot change his identity during a session. Re-authentication is achieved using the SMA Cert. After authentication, the SMA is issued a certificate to become SMA Cert, this new MA will then be used for re-authentication with ASSA Cert. As long as the certificate of SMA Cert is valid, the supplicant will continue to have access to the network. If for any reason the certificate of SMA Cert becomes invalid, the network port on the authenticator opens and the supplicant is disconnected from the network. A similar scenario exists for roaming clients or supplicant. When a supplicant roams from one access point to another, the SMA Cert carries out re-authentication of the supplicant on the new authenticator. If the certificate of the SMA Cert is valid, the supplicant continues to have network access otherwise the network is disconnected **Figures 7** and **8** shows the re-authentication process and agent migration process during roaming.

6.3. Security Issues in MA Scheme

A lot of research efforts have been devoted to the security of MA and platforms with a view to making agent based solution attractive. In order to provide adequate security for the gents and platforms, the Secure and Open Mobile Agent was considered. SOMA architecture protects both the execution sites and the agents [11]. SOMA addresses the problem of protecting MA while executing in malicious sites. To grant the agent integrity, several solutions are fully integrated in SOMA, aimed at detecting any attacks targeted to modify or delete the agent state.

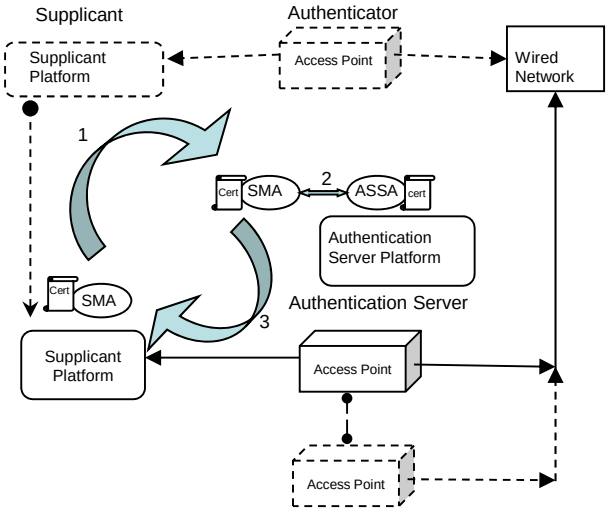

Figure 7. MAWAA migration process during roaming.

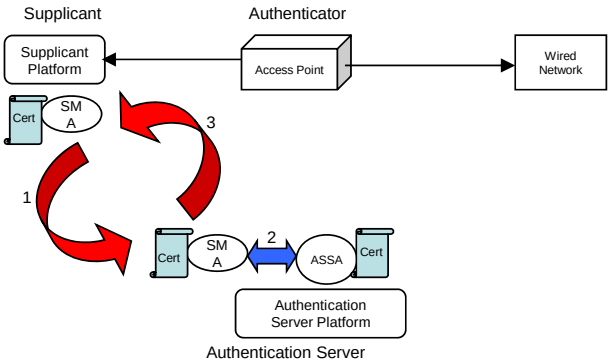

Figure 8. MAWAA re-authentication process.

6.4. Proposed Mobile Agent Platform

The Aglets Software Development Kit is an environment for programming MA in Java. The aglet is able to execute, halt its execution on one host, dispatch itself to another host, and resume execution there. The aglet is capable of moving both the code as well as the data. The aglet is well suited for the internet environment. The proposed mobile agent platform is listed below.

- ASDK free software by IBM
- Latest version is 2.0.2
- Good GUI
- Very accessible
- Good documentation
- Implemented standards; MASIF, and CORBA
- Communication; Message passing between agent, socket
- Mobility; Java serialization
- Security policy; built in security mechanism

7. Conclusion and Future Work

This paper provides a way to have a secure transmission

in wireless network. We proposed the use of mobile agents to provide dependable Internet services delivery to users. The importance of security in a wireless network environment cannot be over emphasized. This is due to the fact that the transport medium is shared, making it difficult to provide effective physical security controls to restrict access to the network. As a result, strong access control and authentication become necessary to provide adequate security.

Unfortunately, 802.1× authentication and key management have some flaws in the composition of the protocol. We have proposed the mobile agent approach to solve the inherent security flaws in 802.1× authentication protocol. Hence we have designed the Mobile Agent Wireless Authentication Architecture (MAWAA) as a solution to some security issues in wireless networks. Future research will focus on the following security issues relating to MA which includes:

- Confidentiality
- Integrity
- Availability and
- Anonymity

REFERENCES

[1] J. Zhu and J. Ma, "A New Authentication Scheme with Anonymity for Wireless Environments," *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 1, 2004, pp. 231-235.

[2] W. A. Arbaugh, "Wireless Security Is Different," *Magazine of IEEE Computer Society*, *Computer*, Vol. 36, No. 8, 2003, pp. 99-101. http://dx.doi.org/10.1109/MC.2003.1220591

[3] H. Yang, F. Ricciato, L. Songwu and L. Zhang, "Securing a wireless world," *The Proceedings of IEEE*, Vol. 94, No. 2, 2006, pp. 442-454. http://dx.doi.org/10.1109/JPROC.2005.862321

[4] S. P. Alampalayam and A. Kumar, "An Adaptive Security Model for Mobile Agents in Wireless Networks," *IEEE Global Telecommunications Conference*, Newark, 1-5 December 2003, pp. 1516-1521.

[5] L. Vasiu and Q. H. Mahmoud, "Mobile agents in Wireless Devices," *Magazine of IEEE Computer Society*, *Computer*, 2004, Vol. 37, No. 2, pp. 104-105. http://dx.doi.org/10.1109/MC.2004.1266304

[6] W. Arbaugh, N. Shankar, Y. Wan and K. Zhang, "Your 802.11 Wireless Network Has No Clothes," *IEEE Wireless Communication*, Vol. 9, No. 6, 2002, pp. 44-51. http://dx.doi.org/10.1109/MWC.2002.1160080

[7] A. Karnik and K. Passerini, "Wireless Network Security—A Discussion from a Business Perspective," *Proceedings of IEEE Wireless Telecommunications Symposium*, Nicosia, April 2005, pp. 261-267.

[8] A. Mishra and W. A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1× Standard," Report No CS-TR-4328, 2002. http://www.cs.umd.edu/~waa/1x.pdf

[9] J. White, "Mobile Agents White Paper," General Magic, Inc., 1996. http://citeseer.ist.psu.edu/white96mobile.html

[10] D. Lange and M. Oshima, "Seven Good Reasons for Mobile Agents," *Communications of ACM*, 1999, Vol. 42, No. 3, pp. 88-89. http://dx.doi.org/10.1145/295685.298136

[11] A. Corradi, R. Montanari and C. Stefanelli, "Security No.s in Mobile Agent Technology," *Proceedings of 7th IEEE Workshop on Future Trends of Distributed Computing Systems* (*FTDCS*'99), Cape Town, December 1999, pp. 3-8.

[12] N. Borselius, "Mobile Agent Security", *Electronics and Communication Engineering Journa*l, Vol. 4, No. 5, 2002, pp. 211-218. http://dx.doi.org/10.1049/ecej:20020504

[13] H. Aouadi and M. B. Ahamed, "Modile Agents Security," *2nd International Conference on Mobile Technology, Applications and Systems*, Guangzhou, November 2005, pp. 1-6.

[14] Y. Wang, C. Wang and L. Cheng-Horng, "Mobile Agent Protection and Verification in the Internet Environment," *Proceedings of 4th International Conference on Computer and Information Technology*, Wuhan, September 2004, pp. 482-487,

[15] N. Aboudagga, M. T. Refaei, M. Eltoweissy, L. A. Dasilva and J. Quisquater, "Authentication Protocols for Ad Hoc Networks: Taxonomy and Research No.s," *Proceedings of* 1*st ACM International Workshop on QoS and Security in Wireless and Mobile Networks*, Montreal, October 2005, pp. 96-104.

