Multi-Agent Systems in Quantum Security for Modern Wireless Networks

Xu Huang and Dharmendra Sharma

Faculty of Information Sciences and Engineering,
University of Canberra, ACT 2601, Australia
{Xu.Huang,Dharmendra.Sharma}@canberra.edu.au

Abstract. Security in wireless networks has become a major concern as the wireless networks are vulnerable to security threats than wired networks. The 802.11i wireless networks uses 4 way handshake protocol to distribute the key hierarchy in order to encrypt the data communication. In our previous research work [2], [3], we have investigated Quantum Key Distribution (QKD), for key distribution in 802.11 wireless networks. The whole communication flow of our proposed protocol can be split into several key processes. It can be seen that these processes can be implemented efficiently using Software Agents. In this paper we shall focus on the use of Software Agents in quantum cryptography based key distribution in WiFi wireless networks.

1 Introduction

Wireless communications are becoming ubiquitous in homes, offices and enterprises with its ability to provide high-speed, high-quality information exchange between portable devices.

WiFi networks uses 802.11 and 802.1X for association and authentication process. The authentication of the end users is essential in wireless networks as the wireless medium is accessible openly. A lot of research papers highlighted the security flaws of wireless networks based on 802.11 [10], [11], [12], [13]. Most of those are happening in the form of Denial of Service (DoS) attacks, Main-in-the-Middle (MiM) attacks, session hijacking (SH) etc.

In our previous [2], [3] and subsequent work, we have come up with a novel protocol to perform the key management in WiFi networks. Software agents can deliver much needed intelligent behavior to WiFi networks especially in case of adversary attacks. In this paper, we explain how Multi Agent Systems (MAS) can be used to perform the key exchange in WiFi networks.

2 Integrating Quantum Key Distribution in IEEE 802.11i Networks

The IEEE 802.11 Task Group has come up with an amendment to the IEEE 802.11 standard [4] called IEEE 802.11i [1] in 2004 to address the security flaws encountered

J.D. Velásquez et al. (Eds.): KES 2009, Part II, LNAI 5712, pp. 119–126, 2009.

in its initial design. IEEE 802.11i separates the authentication and encryption key management. For authentication 802.11i uses IEEE 802.1X [5], [6] and pre-shared key. IEEE 802.1X offers an effective framework for authenticating, managing keys and controlling user traffic to protect large networks.

Once this process completes, the 802.11i 4-way handshake process takes place and ensures the 802.11i key hierarchy to establish at both ends. This key hierarchy consists of several keys, namely: Pairwise Master Key (PMK), EAPOL-Key Confirmation Key (KCK), EAPOL-Key Encryption Key (KEK), Group Temporal Key (GTK) and Temporal Key (TK).

2.1 Wireless with Using of Quantum Cryptography

Though the use of quantum cryptography in wireless communications is still premature, the "unconditional security" [19] of quantum cryptography offers much needed security for wireless networks. At present lot of research work and commercial implementations are happening in this area [17], [18], [23], [24]. Several QKD protocols such as SARG04 [7], BB84 [8], B92 [9] and six-state [10] exist as of now. Out of those, BB84 has proven in practical networks. SARG04 protocol is an improved version of BB84 by eliminating Photon Number Splitting (PNS) attacks. As BB84 does, SARG04 protocol operates in two stages: Quantum channel and Classical channel. In the first stage, photon transmission takes place via quantum channel between two parties. Each of these photons represent a binary bit value of the secrete key. During the second stage, the two parties communicate with each other as per the SARG04 protocol to obtain the secrete key. The second stage comprises of four main phases: (1) Raw Key Extraction (Sifting), (2) Error Estimation, (3) Reconciliation and (4) Privacy Amplification. Further investigation of SARG04 protocol is beyond the scope of this paper.

2.2 QKD Based Key Exchange in 802.11i

Figure 1 shows the full 802.11i protocol communication including the quantum key exchange. Flows 1 to 6 illustrate the IEEE 802.11 association and authentication process. During this process, the Supplicant creates an 802.11 association with the Authenticator. Once the IEEE 802.11 association is completed, the IEEE 802.1X authentication starts with the Supplicant sending EAP-Start message to the Authenticator. This process is shown by flows 7 to 13 of Figure 2. In our work, we choose to use EAP types such as EAP-TLS, EAP-TTLS etc. that offer mutual authentication between the Supplicant and the Authenticator.

At the end of this process, i.e. flow 13 of Figure 2, both Supplicant and Authenticator are in possession of Pairwise Master Key (PMK). Then the communication switches to quantum channel and the photon transmission takes place from the Supplicant towards the Authenticator. Once the quantum transmission finishes, communication channel switches back to wireless channel. Afterwards the SARG04 protocol takes place as shown in flows 15 to 18 in Figure 2 to obtain the final secrete key. From this key, the 802.11i key hierarchy containing PTK, KCK, KEK, TK and GTK can be retrieved. The TK is used to encrypt data for the subsequent data communication. This whole process is not explained in detail in this paper as our focus is on the use of agents for this protocol.

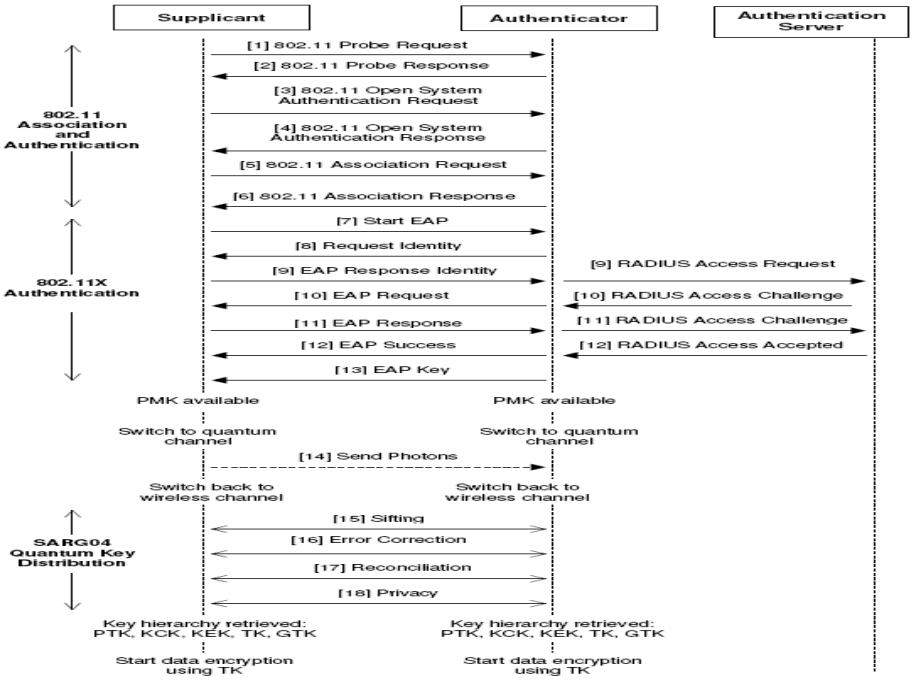

Fig. 1. he QKD based Protocol for Key Exchange

3 Implementation of Agent-Based QKD in WiFi Networks

3.1 Why Multi Agent System?

An Agent can be referred to as a sophisticated computer program, which is capable of acting autonomously to accomplish tasks on behalf of its users, across open and distributed environments. Hence agents have individual internal states and goals, and they act in such a manner as to meet its goals on behalf of its users [20]. Multiple agents can work together to form a multi-agent system (MAS), which offer many advantages over a single agent or centralized approach [16].

Multi Agent Systems in our quantum based key distribution in IEEE 802.11i networks has various advantages. Firstly, the whole protocol can be subdivided into smaller independent modules: 802.11 Association, 802.1X Authentication, Quantum Communication and SARG04 key extraction. These sub-modules can be represented by individual agents to accomplish the main task required. By this way the workload can be distributed among the sub-modules, rather than handling by a single piece of software (centralized approach). Secondly, there are different varieties of EAP types in use for 802.1X authentication such as EAP-TLS, EAP-TTLS, PEAP etc. Therefore, rather than having separate communication flows for each of them, wrapper agents can be used to implement those different EAP varieties. Thirdly, the system maintenance becomes easy as the agents can work independently. Whenever a new change is

required to the protocol, it can be done without effecting to the other modules. Fourthly, the system is open to extensions due to modularization via agents. For example, imagine a case where a new EAP type introduced to the protocol suite. In such instances, it can be easily incorporated into the agent society via another agent.

Agents also offer the intelligent behavior to the system. This is a special feature where other wireless protocol implementations are lacking. With this feature, the agents can be taught to detect possible adversary attacks.

3.2 802.1X Protocol Standards and Possible Attacks on 802.11

Many research papers have shown security vulnerabilities of 802.1X standard [14]. As an example, we shall discuss two such attacks.

Session Hijacking: It was shown that session hijacking is possible on 802.1X [14]. This is shown in Figure 2. In these types of attacks, an adversary can spoof communication between a legitimate supplicant and the Authenticator till EAP Success message is received. At this point the adversary sends 802.11 MAC disassociate message using Authenticator's MAC address. This causes the legitimate Supplicant to get disassociated from the Authenticator. However, at this moment the Authenticator is not aware that the legitimate supplicant has kicked out, so it still remains in Authenticated state. The adversary takes this opportunity to hijack the session.

Denial of Service Attacks: Both 802.11 and 802.1X protocols are subject to DoS attacks [14]. These DoS attacks happen in several ways. Adversaries can send fake EAPOL Logoff, EAPOL Start and EAP failure messages towards Authenticator causing the system to fail.

3.3 QKD Based MAS Application

In our approach, we split the main functionalities of each of the major phases to be represented by software agents. As identified before, the authentication and key establishment can be split into following main components:

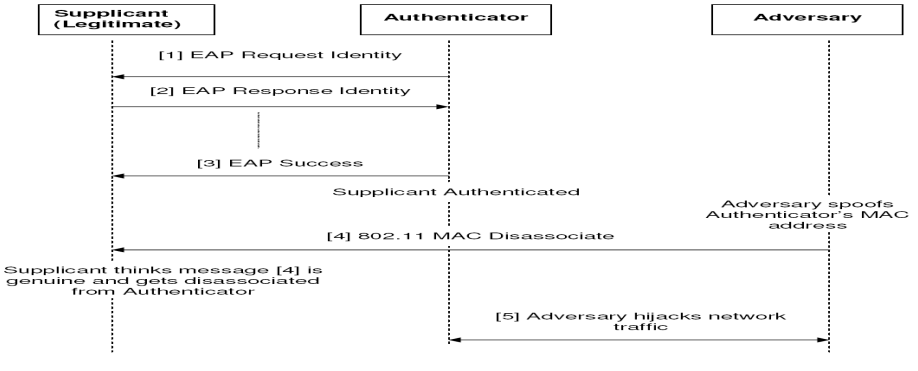

Fig. 2. Session Hijack by MAC address Spoofing

- 802.11 Association and Authentication: for the supplicant to associate with the switch
- 802.1X Authentication: to facilitate mutual authentication between Supplicant and Authenticator
- Quantum transmission: send photons to Authenticator to be used for the key
- Key recovery using SARG04 protocol: recover the final key by removing errors

In our approach, the Agent Society is made up of a main Enterprise as shown in Figure 3 – *The Enterprise*.

Supplicant by executing 802.11 and 802.1X protocols. To facilitate the services, Authenticator spawns a new enterprise for each Supplicant that enters into the wireless network. At the same time the Supplicant too creates one instance of this enterprise to proceed with the communication. Single instance of the enterprise is sufficient at the Supplicant's end as it is only dealing with one Authenticator at a time. These enterprises get together makes the overall Agent Society spanning across the WiFi network served by the Authenticator as shown in figure 3-*The Agent Society*.

802.11 Agent: The main aim of this agent is to perform the 802.11 Association and Authentication. In doing so, this agent can deliver something present 802.11 standard is not capable of doing. That is, with the use of artificial intelligence, this agent is able to take decisions during various adversary attacks.

802.1X Agent: This agent carries out the 802.1X authentication. In this implementation, for simplicity, we only focus on EAP methods that support mutual authentication. This agent is able to support multiple EAP protocols by communicating with different wrapper agents. In addition, it is also able to make decisions on suspicious messages from adversaries similar to what 802.11 Agent does.

Quantum Communication Agent: This agent communicates with hardware devices such as photon transmitter and receiver to make the quantum transmission happen.

SARG04 Agent: The main task of this agent is to execute the SARG04 QKD protocol. It executes the 4 phases of SARG04 protocol in order to extract the final secrete key.

Coordination Agent: The coordination agent communicates with all other agents within the enterprise. Coordination agent in each communication session assures that monitoring efforts and management of internal requests with other agents handled consistently within that specific session.

In this solution, not a single agent is fully aware of the whole communication process. Instead, all agents get together to make the whole communication happen. With this kind of approach, which is quite suitable to be represented as an agent society, modifications can be done effectively.

Similarly, the DoS attack described in above section can be dealt with when 802.1X Agent detects any fake EAP messages.

The software test bed is now being implemented on two computers with one acting as the Supplicant and the other as Authenticator.

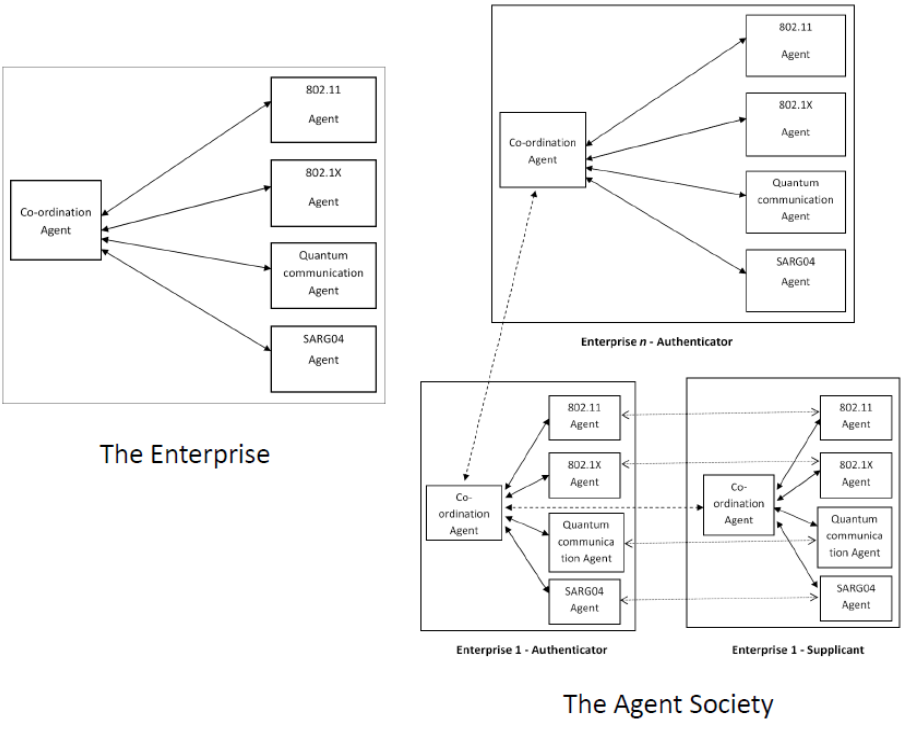

Fig. 3. The Enterprise and The Agent Society

Since the "Native WiFi" software developments are based on C++ platform, we have concentrated on developing MAS application using the same C++ language. We have found that most of the MAS applications only support Java based developments.

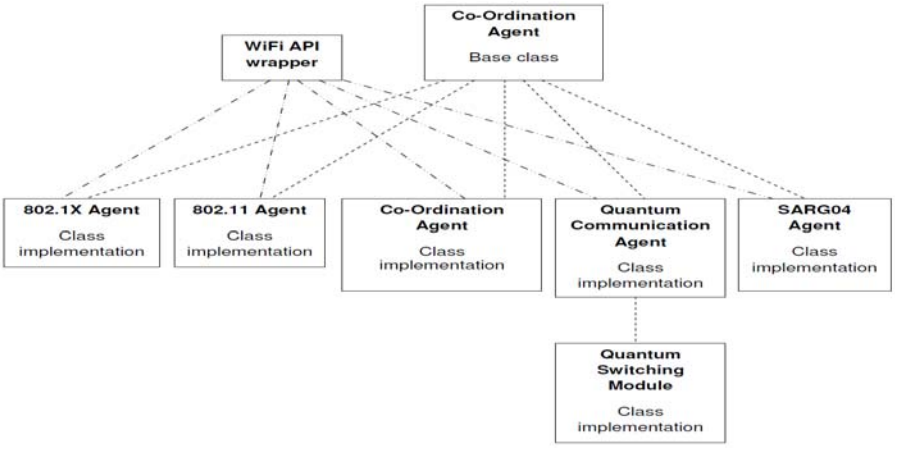

Fig. 4. High level C++ class diagram of the MAS application

Therefore we have decided to write our own application for MAS using C++. This works well with MAS, since C++ being an object oriented language, the agents can easily be represented by C++ classes. As of now we are in the process of developing the SARG04 Agent along with Co-ordination Agent. Appleby and Steward of BT Labs have done a similar approach to prototype a mobile agent based system for controlling telecommunication networks [25].

In this MAS application, we implement C++ class structure to reflect the mobile agents as per the Figure 2. The Co-ordination agent acts as the main class (or agent), which gets created when a Supplicant requires WiFi service. Co-ordination agent calls the other agents only when their service is required. High level C++ class diagram of the MAS application is shown in Figure 4.

4 Conclusion

In this paper we have discussed the use of software agents in QKD based key distribution protocol in WiFi networks. This agent society is particularly useful at Authenticator side as it plays a key role within WiFi networks. As the Authenticator assigns a separate enterprise to look after each Supplicant, the work load can be distributed. This is one of the key requirements for Multi Agent Systems.

This agent approach provides lot of advantages to the wireless communication. Since the key work flows are incorporated into agents, maintenance too becomes easy. Whenever new change to the protocol is needed, it can be done with less effort, without affecting the other agents. It also provides extensibility by allowing different EAP wrapper agents to facilitate different EAP types.

Thus we can conclude that the use of Multi Agent Systems in QKD based WiFi networks offer lot of benefits. There are other research works being done in WiFi area using software agents [21]. We believe our approach using Multi Agent Systems will contribute to develop secure communications for future wireless networks.

References

1. IEEE Std 802.11i, IEEE Standard for Information Technology – Telecommunication and information exchange between systems – Local and metropolitan area networks – Specific requirements. Part 11, Security Enhancements (2004)
2. Huang, X., Wijesekera, S., Sharma, D.: Implementation of QKD in 802.11 Networks. In: Proceeding 2009 IEEE International Conference on Networks Security, Wireless Communications and Trusted Computing, vol. 2, p. 125 (2009)
3. Wijesekera, S., Huang, X., Sharma, D.: Multi-Agent Based Approach for Quantum Key Distribution in WiFi Networks. In: Håkansson, A., et al. (eds.) KES-AMSTA 2009. LNCS (LNAI), vol. 5559, pp. 293–303. Springer, Heidelberg (2009)
4. ANSI/IEEE 802.11, 1999 edn (R2003), Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (2003)
5. IEEE Std 802.1X, IEEE Standard for Local and metropolitan area networks, Port-Based Network Access Control (2004)
6. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H.: RFC – 3748, Extensible Authentication Protocol, EAP (2004)

7. Scarani, V., Acin, A., Ribordy, G., Gisin, N.: Quantum cryptography protocols robust against photon number splitting attcks (2004)
8. Bennett, C.H., Brassard, G.: Quantum cryptography: Public-key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, pp. 175–179 (1984)
9. Bennett, C.H.: Phys. Rev. Lett. 68, 3121 (1992)
10. Bruß, D.: Optimal Eavesdropping in Quantum Cryptography with Six States. Physical Review Letters 81, 3018 (1998)
11. He, C., Mitchell, J.C.: Analysis of the 802.11i 4-way Handshake
12. De Rango, F., Lentini, D., Marano, S.: Statis and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i (June 2006)
13. He, C., Mitchell, J.C.: Security Analysis and Improvements for IEEE 802.11i
14. Mishra, A., Arbaudh, W.A.: An Initial Analysis of the IEEE 802.1X Standard (February 2002)
15. Leavitt, N.: Will IEEE 802.1X Finally Take Off in 2008?, pp. 82–85. IEEE Computer Society, Los Alamitos (2008)
16. Multi-Agent Systems, http://www.cs.cmu.edu/~softagents/multi.html
17. SECOQC, Development of a Global Network for Secure Communication based on Quantum Cryptography, http://www.secoqc.net/
18. Graham-Rowe, D.: 'Quantum ATM' rules out fraudulent web purchases, New Scientist, Magazine (2629) (November 2007)
19. Mayers, D.: Unconditional Security in Quantum Cryptography. Journal of the ACM 48(3), 351–406 (2001)
20. Software Agents: An Overview, Hyacinth S. Nwana, Intelligent Systems Research, AA&T, BT Laboratories (1996)
21. Automatic Resumption of Streaming Sessions over WiFi Using JADE, Alvaro Suárez, Member, IAENG, M. La-Menza, Elsa M. Macías, Member, IAENG and Vaidy Sunderam
22. Genesereth, M., Fikes, R.: Knowledge interchange format. Version 3.0 Reference Manual, Tech-nical Report Logic 92-1, Computer Science Department, Stanford University (1992)
23. http://www.idquantique.com/ id Quantique, Quantum Cryptography
24. New Scientist, Quantum ATM rules out fraudulent web purchases, November 10 (2007)
25. Appleby, Steward: Mobile Software Agents for Control in Telecommunications Networks. BT Technological Journal 12(2), 1040113 (1994)