American Journal of Language, Literature and Culture
1(1):29-35, August 2019

Development of an Anonymous Key Exchange System for Roaming Services

Thompson Aderonke, **Akinsowon Omoyele**, **Alese Boniface Kayode**
Department of Computer Science, The Federal University of Technology, Akure, Nigeria

Abstract
The development of an anonymous key exchange system for roaming services is highly desirable to wireless users, but ensuring the security and efficiency of this process is challenging. The main issues have always been to secure the channels of communication and data from eavesdroppers and hackers. This research paper therefore focuses on the basic security concerns for establishing channels of communication between users and servers and proposes and implements a better method. This work is implemented using Visual Studio C# to develop a roaming application that allows the user to hop from networks to stronger networks.
Keywords: Roaming, Anonymous Key Exchange, Home server, Foreign server

1. Introduction

In this present world of technologically advanced Computer Networks and Telecommunications system, user mobility has become an increasingly important feature. User mobility refers to a situation in which a user subscribed to a network in his or her own environment, can change to a different geographical location where the home servers' network does not reach but the user can access the services of a totally different operator. [YWD07]. This phenomenon is called roaming. Traditionally, roaming is a handing over from one server (home server) to another (foreign/visited server) even when the two networks may not be the same type in order for a user to continue to get access to network services. So, users can be transferred from their home server to a foreign server seamlessly.

The advantage of roaming is that users can have unlimited access to network services and a much broader network coverage and not be limited to that of their home servers alone. Roaming can be between different network devices. Roaming from a wireless local area network (WLAN) and a mobile network and vice versa is a good example. [Lam86]

1.1. Roaming

Typically, roaming involves three parties, namely; the roaming user, the home server to which the user is subscribed to and the foreign or visited server. Before a user can access a foreign server, there has to be an agreement between it and the home server. The user is granted access to the foreign server's resources only after an agreement is reached and the authentication process has been carried out. As a result of these developments, user privacy has become a top-notch security issue, especially in order to prevent unauthorized users from access. Generally, most users prefer to keep their real identity from eavesdroppers, even from the foreign server itself. An exposure of users' identity can lead to further exposure of the users' session for any time; whether the past or future. The method of hiding the users' identity is called User Anonymity. Furthermore, it is of utmost importance that a user's movement cannot be monitored or traced all through. Disclosure of a user's identity can allow unauthorized persons to monitor his/her sessions and location. Gaining access to a user's location without consent is outright violation of user privacy. The process in which no other party can identify previous sessions and protocol run except the user alone, not even the foreign server is called User Untraceability.

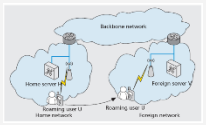

Figure 1. Network Roaming

As part of the needed modes to protect transmission, data confidentiality and data integrity are very much vital. Data confidentiality ensures that no other party gets access to the data exchanged between the user and the foreign server. Even the home server does not have access to this because data exchange is strictly between the user and the foreign server. The only function the home server is needed is for user authentication. Data integrity ensures that the data exchanged is not tampered with by third parties, that is, the very data sent by the foreign server is the exact one secured by the user. Hence, this work explores in details the design of a key exchange system between the user and the foreign server which will ensure anonymity for the user.
Uninterrupted and unhindered roaming are very key factors in the modern day 21st century but security and user privacy can make it very challenging. Although the same may be said for all communication systems, roaming services have special requirements and vulnerabilities, therefore deserve special attention. Lots of protocols have arisen to solve this problem but a lot of them have not really done justice to the issue. [HHG10]

1.2. Hypotheses

1. Can users be assured that their identities are concealed for their roaming sessions?
2. Is the communication between users and the foreign servers secure and inaccessible to unwanted parties?

This research is aimed at implementing the data roaming services through the development of an application using Visual Studio C# which automatically switches to the strongest wireless network available to it. The application does not need a total revelation of its identity to connect to the strongest network. It only needs to present the password of the network for connection so that the application can be verified by the network it is visiting.

2. Related Works

What is a key? A key is just a parameter that is used to determine the output of a cryptographic algorithm. The key is very important to the deciphering of the algorithm because without it, the algorithm would be like any other, thereby yielding no useful result. We have the public key and the private key. The public key is a key in cryptography that can be got and used by anyone to encrypt messages in such a way that deciphering is only possible if the recipient has a second key (public key) which will be known to him only. The private key is a secret key that could be used for encryption or decryption by users involved in an exchange protocol. Basically, in cryptography, there are two types of key algorithms; symmetric key algorithms and the asymmetric key algorithms. The symmetric key algorithm uses the same key for both the encryption and decryption of information. This means this particular has to be kept secret and closely guarded from eavesdroppers and hackers else, once it's gotten hold of, they'll be able to decrypt and tamper with the information. The asymmetric algorithm makes of a pair of keys (public and private), one to encrypt the information (public key), and the other to decrypt it (private key).
What is a key exchange system? A key exchange system in cryptography refers to a method through which cryptographic keys (whether public or private) are exchanged between users. These keys enable the user to be involved in the exchange of encrypted messages. While anonymous key exchange system refers to a situation where the users' identity is hidden but can be verified and still go ahead to carry out the exchange.

The basic problem with the key exchange system has always been how to exchange these keys without a third party accessing and decrypting their messages. This problem has given rise to a series of solutions over the past years but a most notable one is the Diffie-Hellmann key exchange method. [YAA06]. In the year 1976, Whitfield Diffie and Martin Hellmann jointly published this scheme. This method allows users without prior knowledge of one another to be able to establish a channel for communications through the establishment of a shared secret key. In order to implement Diffie-Hellmann, there has to be two users willing to communicate, say Steve and Eve. First Steve and Eve agree publicly on a prime modulus and a generator.
Let g=3 and p=17. Then Steve selects a private random number, say 15 and calculates 3^{15} mod 17≡ 6. Then Steve sends this result (6) to Eve. Eve also selects her private random number, say 13 and calculates 3^{13} mod 17≡12 and sends this result (12) publicly to Steve. The trick of the whole scheme is that when either Steve or Eve raises each other's transported results to the power of their private number, they arrive at the same answer.
That is, For Steve: 12^{15} mod 17≡10 and For Eve: 6^{13} mod 17≡10. With this agreed private answer, they can go ahead and share messages since no third party will be able to decrypt their messages without a private key.

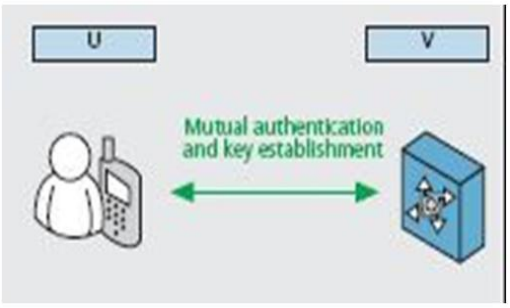

Figure 2. Two-party Authentication Roaming

A lot of research has been done in this field and we have looked at a few of them. Some of the previous works done in this field can be classified into two-party and three-party protocols. The two-party protocols require the involvement of just two parties; the roaming user U, and the foreign server S. This approach totally excludes the involvement of the home network where the foreign server performs the authentication and session key establishment with the roaming user. The advantages are that it helps to avoid loss of connection problems between the foreign server and the home server. Also, this protocol protects the home server from DOS attacks through the foreign server and reduces the number of communication rounds. All of these advantages have led to a continual upsurge of the two-party authentication protocol. However, the two-party authentication roaming is not without its disadvantages. Due to the structure being implemented in this protocol, which requires that the foreign server be able to authenticate the validity of users, complicated algorithms have to be written thereby resulting in high computation overhead.
The three-party protocol basically involves the home server, the roaming user and the foreign server. The user sends a login request to the foreign server; on receiving this request, the foreign server contacts the home server just for authentication. Under this approach, the user is only permitted to connect with the foreign server after it has been authenticated by the home network as part of its networks. It is very suitable for resource limited cases as it does not need too many or too costly infrastructure to set up. However, its downsides are that some of the basic examples like the EAP-MD5, EAP-TLS and so on cannot provide user anonymity and non-traceability.

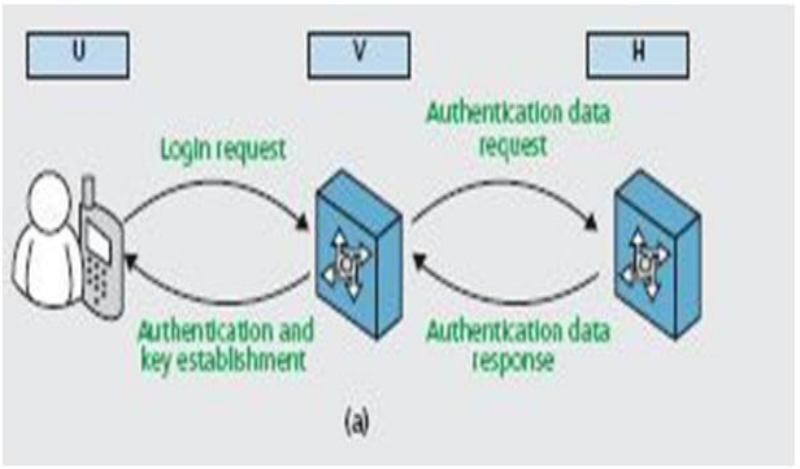

Figure 3. Three-party Authentication Roaming

In (Park et al, 2001), their design was focused on ensuring user anonymity and the freshness of temporary identity in each session. The design was such that when a roaming user needs connection with a foreign server, it presents an alias (a secret random number) and points at a server as its home server. The alias can't be understood by the foreign server and it then presents it to the pointed-out home server. The home server identifies the user to the foreign server and the key session is established. The problem with this design is that the user's identity is made known to the foreign server. This means that the user's progress can be tracked by the foreign server even after the session has being terminated. Also, it has been revealed that the design is vulnerable to an attack called, the deposit-case attack. [PGK01]

Samfar et al, 1995 worked on establishing a session key in each protocol execution between a user and a foreign server. However, the key is known to the user's home server which is one of the main differences between our research work and that of Samfar et al. The first challenge that this method poses is that the session key between the user and the foreign server remains unchanged all through the sessions between them. This will allow the foreign server to easily trace the user. Another issue is that it is also vulnerable to deposit-case attack. [SMA95] Also in 1997, Varadharajan et al proposed a hybrid method whose protocol uses an alias which appears unintelligible to anyone except the home server and it is a technique that is commonly used to provide user anonymity in mobile communications. One of the major trade-offs of this protocol is the fact in order to maintain untraceability; the alias has to be renewed after use every time which eventually results in longer connection time and extra cost. Another problem that results is about the synchronization between the user and the user's home server. If peradventure the communication link between the user and the user's home server is broken or some form of disruption happens, the synchronization may be lost. [VM97] In 1994, Ateniese et al proposed to create a temporary record for the roaming user so that subsequent access would be a lot easier and faster. The major trade-off is that the protocol does not create a way for the roaming user to authenticate the foreign user (being sure of the foreign server's identity is important because of fraudulent servers). Unfortunately, this protocol does not provide key establishment between the roaming user and the foreign server. [AHKT98]

Lee et al divided their Protocol into three processes; the setup process, the online authentication process and the offline authentication process. In the setup process, the user enrolls with the home server and is given a smart card for services. In the online authentication process, when the MS roams into a foreign server, the foreign server authenticates the identity of the user through the home server. In the off-line authentication process, the foreign server can authenticate the roaming user without contacting the home server and requesting further processes. The problem with this method is that the protocol does not offer user anonymity which is supposed to be the aim of the project. Any intruder can obtain the user's public key from the wireless network and obtain the identity. The essence of providing a secure channel between the user and the foreign server is to keep the identity of the user hidden which has not being

fulfilled by this work. Another problem is that the sectional key of the user can be used to track the user's movement by extracting the past session keys. [BGSW00]

3. Proposed Method

There are basically two entities in this protocol; the roaming user which is the application and the foreign server which can be any other wireless network available at that instance. Knowing that AKE means Anonymous Key Exchange, let A and B represent the identities of the user and the server respectively. And let the key pairs of A and B be represented by $(Z_A; P_A)$, $(Z_B; P_B)$ respectively. Z_A and Z_B basically represent the private keys of A and B while the public keys for A and B are represented by P_A and P_B. The hidden identity of A which is one of the main causes of the project is given as [A]. If the generated key is given as Ω, then the Anonymous Key Exchange protocol is given by:

$$\Omega \leftarrow \text{AKE}\ (A, B, (Z_A; P_A), (Z_B; P_B))\ [A].$$

The scope of this SAD is to show the architecture of the Wi-Fi Roaming application developed for the implementation of this work. The Wi-Fi Roam application based on the Windows Presentation Foundation technology by Microsoft was deployed on a Windows-based operating system environment. The system was secured so that a device can connect with any network anonymously.
Hence, the following basic security behaviors were implemented:

- Ÿ Authentication: connecting to existing network using a WPAK-Secure password.
- Ÿ Confidentiality: sensitive data was encrypted (User).
- Ÿ Data integrity: Data sent across the network cannot be modified by a tier.
- Ÿ Persistence: The device will continually check for existing networks to connect to, in order to satisfy its roaming ability.
- Ÿ Reliability/Availability: The availability of the system is an important advancement for users of existing networks, as it is a roaming system. The candidate architecture must ensure failover capabilities. Reliability/Availability was addressed through the WPF platform.

A device accesses the Wi-Fi Roam application and searches for the available networks. The device chooses from the list of networks judging by the strength of signal. Then, the device performs connection request with exchange of key/credentials. Once the key has been validated, device connects to the network, continues background scanning of networks with stronger signal and initiates re-connection to one if found.

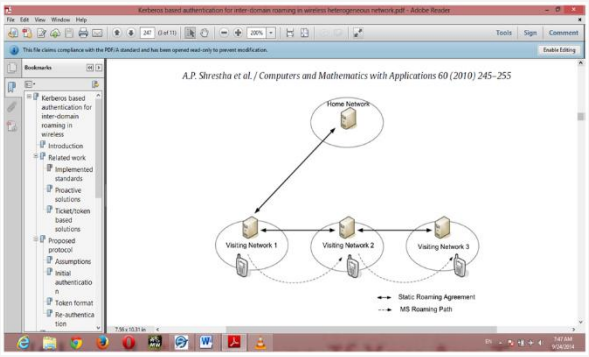

Figure 4. Roaming User Visiting Networks of Various Signal Strengths

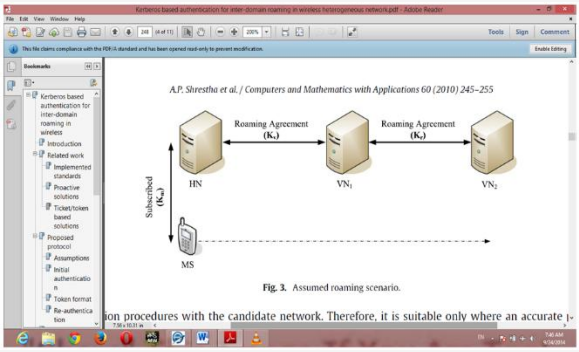

Figure 5. User Home Network Establishing Key Agreement with Visited Networks

The Wi-Fi Roaming application is divided into layers based on the N-tier architecture

Table 1. Wi-Fi Roaming: N-Tier Architecture

Client/Device Layer	Presentation Layer	Authentication Layer	Server Layer
Desktop App WPF	Network Services	Network Access Handshake	Database Internet Access
WPF		Handshake	Internet Access

4. Algorithm Description

4.1. Architectural Layer Dependencies

The layering model of the Wi-Fi Roaming application is based on a responsibility layering strategy that associates each layer with a particular responsibility. This strategy has been chosen because it isolates various system responsibilities from one another, so that it improves system development.
Each layer has specific responsibilities.
Ÿ The presentation layer deals with the presentation logic and the pages rendering.
Ÿ The control layer manages the access to the domain layer.
Ÿ The resource layer (integration layer) is responsible for access to the network information (systems information, databases or other sources of information).
Ÿ The domain layer is related to the server/host and manages the access to the networks.
Ÿ The Common Elements layer gathers the common objects reused through all the layers.
The Wi-Fi Roaming application is quite simple and only contains two basic features, one for the scanning and filtering networks and the other allowing a device to connect to a preferred network. Network services are reused for the network-scanning functionalities.
Microsoft Visual C# was the major tool used in implementing this research work. In the development of the Wi-Fi Roam, there are 5 main horizontal tabs; the AnimationHelper, the ChannelBar, ChannelHeader, MainWindow and the Status Callback. These are all shown in the snapshot below Figure 7.
Ÿ The Animation Helper: It simulates the scanning experience to show the user how foreign networks are scanned.
Ÿ The Chanel Bar: The channel bar tab was developed to show the channels in which the discovered devices lie. It basically has 17 horizontal bars stacked side by side.

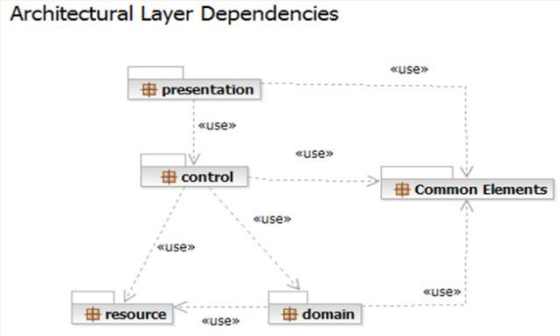

Figure 6. Architectural Layer Dependencies

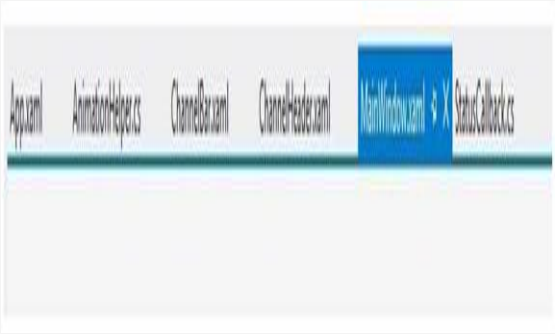

Figure 7. Main Tabs

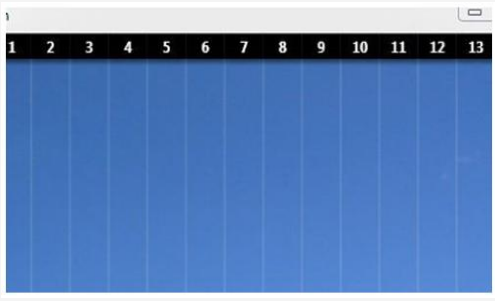

Figure 8. The Channel Bar

```
<UserControl x:Class="WiFiChannelSpread.ChannelBar" x:Name="MyRoot"
             xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"
             xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"
             xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006"
             xmlns:d="http://schemas.microsoft.com/expression/blend/2008"
             mc:Ignorable="d" VerticalAlignment="Stretch" HorizontalAlignment="Stretch"
             d:DesignHeight="200" d:DesignWidth="40"
             MouseEnter="MyRoot_MouseEnter" MouseLeave="MyRoot_MouseLeave">
    <Grid>
        <Rectangle Name="StaticBar" Opacity="0" HorizontalAlignment="Stretch" VerticalAlignment="StretcH
            <Rectangle.Fill><ImageBrush ImageSource="Images/Static.png" Stretch="Fill" /></Rectangle.Fi
        </Rectangle>
        <Border Name="BorderRect" BorderBrush="White" BorderThickness="1,0,1,0" VerticalAlignment="Stret
    </Grid>
</UserControl>
```

Figure 9. Code for the Channel Bar

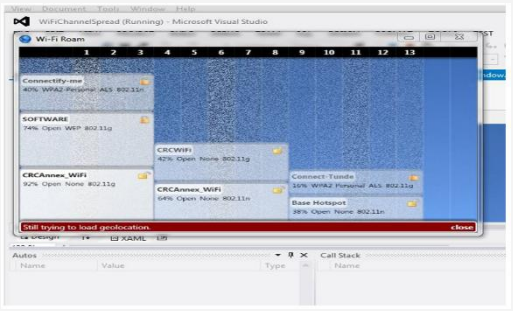

Figure 10. Networks available and within range

5. Result and Discussion

At the end of implementation, the application was able to search for network around, record the percentage of strength of the networks and switch to the strongest network. This roaming application reduces the stress that users have to go through to manually search for networks before connecting to the available ones. It automatically searches for the available networks for connection even while the user is connected to another network. This is done so that when the user disconnects or leaves the network coverage, it will be easy to connect to other networks. It also protects the user's identity all through the period of roaming. This however can only be done after the user has been authenticated for connection to the foreign network. The application establishes a key with the foreign server in order to give a secure channel for communication, making sure that only authorized parties have access to them.

6. Conclusions

In this work, focus was on anonymous roaming from network to network and trying to keep the identity of the users from eavesdroppers and hackers. Roaming services on wireless networks give people better and uninterrupted access to network services. This process should be fast enough to support demanding applications too.

References

[1] [AHKT98] Giuseppe Ateniesey, Amir Herzbergz, Hugo Krawczykx, and Gene Tsudik. On traveling incognito. 1998.

[2] [BGSW00] Levente Buttyan, Constant Gbaguidi, Sebastian Staamann, and Uwe Wilhelm. Extensions to an authentication technique proposed for the global mobility network. IEEE Transactions on Communications, 48(3): 373–376, 2000.

[3] [HHG10] Dijiang Huang, Xiaoyan Hong, and Mario Gerla. Situation-aware trust architecture for vehicular networks. IEEE Communications Magazine, 48(11), 2010.

[4] [Lam86] L[eslie] A. Lamport. The gnats and gnus document preparation system. G-Animal's Journal, 41(7):73+, July 1986.

[5] [PGK01] Jaegwan Park, Jaeseung Go, and Kwangjo Kim. Wireless authentication protocol preserving user anonymity. In Proceedings of the 2001 Symposium on Cryptography and Information Security (SCIS 2001), volume 26, pages 159–164, 2001.

[6] [SMA95] Didier Samfat, Refik Molva, and N Asokan. Untraceability in mobile networks. In Proceedings of the 1st annual international conference on Mobile computing and networking, pages 26–36. ACM, 1995.

[7] [VM97] Vijay Varadharajan and Yi Mu. Preserving privacy in mobile communications: A hybrid method. In Personal Wireless Communications, 1997 IEEE International Conference on, pages 532–536. IEEE, 1997.

[8] [YAA06] Attila Altay Yavuz, Fatih Alagoz, and Emin Anarim. Himutsis: Hierarchical multi-tier adaptive ad-hoc network security protocol based on signcryption type key exchange schemes. In International Symposium on Computer and Information Sciences, pages 434–444. Springer, 2006.

[9] [YWD07] Guomin Yang, Duncan S Wong, and Xiaotie Deng. Anonymous and authenticated key exchange for roaming networks. IEEE Transactions on Wireless Communications, 6(9), 2007