Credit-Based User Authentication for Delay Tolerant Mobile Wireless Networks

by

Khaled Hatem Almotairi

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2007

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Wireless Internet has become increasingly popular due to anywhere anytime access feature. The Internet architecture was designed underlying the existing of the end-to-end path connection. The promise of wireless Internet networks is to provide roaming users connectivity anywhere anytime. However, quality of service (QoS) is still an open issue in wireless networks, which are characterized by possible intermittent connectivity and large transmission delays, due to user mobility, sparse mobile node distribution, link failures (because of hostile propagation medium), and/or other high-priority traffic.

In this thesis, a credit-based user authentication scheme is proposed for delay tolerant mobile wireless networks. The proposed authentication scheme isolates the uncertain network condition in the high-delay wireless backhaul with high error rate, and accelerates the overall authentication process when the mobile terminal roams in the visited network. Furthermore, an analytical study of overall network performance is presented for the authentication scheme in terms of authentication cost and delay. Simulation results demonstrate that the proposed credit-based authentication scheme reduces the overall real time transaction cost and delay for delay tolerant mobile wireless networks.

Acknowledgements

I would like to express my deepest and sincere gratitude to my supervisor, Professor Xuemin (Sherman) Shen. His valuable support, guidance and encouragement were vital to achieving this degree.

I would also like to extend my appreciation to my thesis readers, Professor Pin-Han Ho and Professor Sagar Naik, for reviewing my thesis and providing valuable suggestions and comments.

Special thank goes to Minghui Shi for his productive discussions and continuous feedback throughout this research. I am deeply indebted to all my colleagues in BBCR group. I am also grateful to the ECE department staff for their kind assistance and cooperation.

Special acknowledgment is due to the Ministry of Higher Education in Saudi Arabia for granting me this scholarship, also for the generous support from the Saudi Arabian Cultural Bureau in Canada.

Finally, I want to thank my wonderful parents, wife, siblings and friends for being patient with me in all their hardships that they incurred in my long absence, and for offering words of wit and encouragements. Many thanks go to everyone who contributed to make my Master's experience exceptional and very enjoyable journey.

To my lovely parents...

Contents

List of Acronyms **x**

1 Introduction **1**

1.1 Problem Formulation 2

1.2 Thesis Outline 3

2 Authentication in Wireless Networks **4**

2.1 Introduction to Authentication 4

2.2 Authentication Mechanism 6

2.3 Objectives of Designing Authentication Protocols 7

3 Credit-Based User Authentication for Delay Tolerant Networks **10**

3.1 Delay Tolerant Networks 11

3.1.1 Background 11

3.1.2 Characteristics of Delay Wireless Tolerant Networks 12

3.1.3 Solutions 12

3.1.4 Integrated all-IP Delay Tolerant Networks 14

3.2 Related Works 14

3.3 Research Objectives 16

3.4 Credit-Based Authentication Architecture 16

3.4.1 Authentication Credit 19

4 Performance Analysis of Credit-Based Authentication Scheme 20

4.1 Cost Analysis 20

4.1.1 Average Overhead Cost 23

4.1.2 Average Credit Time 24

4.2 Delay Analysis 24

4.2.1 Average Authentication Delay 26

4.2.2 Distribution of Authentication Delay 27

5 Simulation Results 29

5.1 Cost Evaluation 29

5.2 Delay Evaluation 32

5.3 Estimating Credit Time T_i^{credit} 34

6 Conclusion and Future Works 36

6.1 Conclusion 36

6.2 Future Works 37

List of Tables

5.1 Parameters for Simulation Results 30

List of Figures

2.1 Authentication process 8

3.1 Delay tolerant integrated mobile wireless networks 15

3.2 Flow chart of proposed credit-based authentication scheme 18

4.1 Mobile user roaming 22

5.1 Overhead cost vs. authentication credit expiration 31

5.2 Average authentication time vs. authentication credit expiration 32

5.3 Average authentication delay vs. service utilization factor 33

5.4 Probability of the authentication delay distribution 35

List of Acronyms

QoS	Quality of service
WLAN	Wireless Local Area Network
MAN	Metropolitan Area Network
WiMax	Worldwide interoperability for Microwave access
WEP	Wired Equivalent Privacy
ECC	Elliptic Curve Cryptography
HN	Home Network
MT	Mobile Terminal
TCP	Transmission Control Protocol
RTT	Round-Trip Time
IPN	InterPlanetary Network
DTN	Delay Tolerant Network
IRTF	Internet Research Task Force
DTNRG	Delay-Tolerant Networking Research Group
LTP	Licklider Transmission Protocol
MIP	Mobile Internet Protocol

BH	Backhaul Hub
HTTPS	HyperText Transport Protocol Secured
FN	Foreign Network
AP	Access Point
AC	Authentication Credit
FA	Foreign Agency
HA	Home Agency
ACID	Authentication Credit Identification
ID_M	Identification of the mobile terminal
Sig_F	Digital signature signed by the foreign agent
FCFS	First Come First Served
CAC	Call Admission Control
ID	Identification

Chapter 1

Introduction

In the past decade, the development of wireless communication technologies made the Internet ubiquitously. There are a number of wireless technologies such as broadband wireless, 3G network; however, wireless local area networks (WLANs) have become more popular than the others because of the availability of the unlicensed spectrum of WLANs. Moreover, the increasing use of laptops, tablets, and personal digital assistants (PDAs), and the decreasing cost of WLAN equipment, such as access points (APs), made WLANs ubiquitous. The WLANs are based on IEEE 802.11 standard [1, 2]. Thus, the low cost, high capacity, easy deployment, and the speed of wireless networks have pushed clients and small companies to create wireless networks instead of wired networks. Developing wireless Internet access over long distance is potentially to be invested [3]. Wireless metropolitan area networks (MANs) based on IEEE 802.16 (worldwide interoperability for microwave access or WiMax[4]) are currently under deployment and expected to be born soon. Not only WiMax is created for metropolitan wide-area wireless backhaul network, but also it can be used for coverage extension by integrating it with other networks such as Wi-Fi routers and relay stations.

Compare to wireline counterparts, wireless access introduces more challenges to security due to the nature of open medium. In order to provide secure wireless medium, authentication is used as a basis to authorize the mobile terminals and exchange secret keys.

The advantage of wireless networks is to provide roaming users with connectivity anywhere anytime. However, providing quality of service (QoS) in wireless networks is still an open issue, which involves dynamic capacity, traffic load, and network topology. The characteristics of wireless networks are high error rates, long transmission delays, and link failures.

1.1 Problem Formulation

Providing QoS in wireless networks has known to be an important but difficult task. One of the QoS metrics is transmission delay. User authentication information is delay sensitive because it requires real time transaction. Re-authentication causes undesired authentication process in delay tolerant network (DTN). Delay tolerant network will cause unfavorable high latency in user authentication process. Repetition of waiting time before accessing the network can be annoying enough to mobile users. Therefore, minimizing authentication delay is important to achieve acceptable user experience without introducing more overhead to the network.

Thus, in this thesis, a credit-based user authentication scheme for delay tolerant mobile wireless networks is proposed to minimize authentication delay. The proposed scheme pre-authorizes the mobile users based on the credit record after a successful user credit check. The benefit of the proposed credit system is that the full authentication is always performed in the background to keep potential service loss to the minimum, which greatly reduces the overall authentication latency with poor network condition. Furthermore, this proposed scheme can be implemented distributively, so multi-point localized authentication mechanisms can be used to cope with the wireless front end at the foreign network side.

1.2 Thesis Outline

The remainder of this thesis is organized as follows. Chapter 2 presents an overview of the authentication process in wireless networks. A brief introduction about delay tolerant networks and the proposed authentication scheme for delay tolerant mobile wireless networks are given in chapter 3. Chapter 4 presents the analytical model for evaluating the resultant cost and delay of the proposed scheme. Performance evaluations are provided in Chapter 5. Finally, Chapter 6 gives conclusions and suggests further research directions.

Chapter 2

Authentication in Wireless Networks

The employment of wireless technologies has opened big markets worldwide. Thus, achieving secure wireless access is a very important requirement. In this chapter, we present a general overview of authentication in section 2.1. A brief introduction about authentication mechanism is given in section 2.2. Finally, the considerations relevant to the design of effective good authentication protocols are provided in section 2.3.

2.1 Introduction to Authentication

Authentication is defined as the process to identify legitimate users from others. There are three parties in this process: users, home networks (HN), and foreign networks (FN). Authentication process initiates from the users by requesting access to the foreign networks. The foreign networks have to identify and authorize the requested users by negotiating with their home networks. The home networks identify the legitimate users from the others.

The responsibilities of authentication process can be summarized in the following points:

- Block unauthenticated information that may be malicious.
- Prevent illegitimate users to access network rescouses.
- Keep tracking of users' activities.
- Make integration between/among networks easier.

Therefore, the authentication process is basically based on negotiations by exchanging messages. The users have to submit their credentials to the foreign networks to prove their legitimacies. Based on credentials of the users, authentication protocols can be classified. There are two main classifications of authentication: symmetrical shared secret keys and asymmetrical shared secret keys. Both of them have advantages and disadvantages.

Symmetrical authentications are defined as an authentication process based on reconfigured shared secret keys between/among parties. These shared secret keys are used to encrypt and decrypt parties' information. Password authentication [5] and Challenge/response authentication [6, 7] are examples of symmetrical authentications. Symmetrical authentications are more efficient in terms of computations, but less scalable. IEEE 802.11 uses Wired Equivalent Privacy (WEP) as security and authentication protocols for WLANs [8]. IEEE 802.11 as a standard was ratified in September 1999. Two years later, WEP has been shown several security serious flaws [9]. WEP has two authentication modes: Open and closed authentications. The open system authentication means WEP is off—which is already considered as insecure. Since the shared key authentication is not mutually authenticated, only users authenticate to the network. Unfortunately, both of these authentication methods have known to be failed [10].

On other hand, asymmetrical authentications are defined as the authentication process based on public/private keys between/among parties. The sender uses the receiver's public key to encrypt the information and the receiver uses its private key to decrypt the received information. RSA [11] and Elliptic curve cryptography (ECC) [12] are examples of asymmetrical authentications. Asymmetrical authentications are less efficient in terms of computations, cause more power consumptions, but more scalable.

2.2 Authentication Mechanism

In section 2.1, a brief introduction about authentications was presented. The focus of this thesis is on integrated wireless networks. In integrated networks, a home network of a mobile terminal (MT) is defined based on a pre-agreement. When the MT wanders into a FN, the FN has to check the MT identity by contacting its HN. Figure 2.1 shows the authentication mechanism that has two dimension charges, overhead cost and delay. The effect of authentication on network performance can be easily seen in Figure 2.1. As the number of (re)authentications increases, the overhead increases. In this work, the overhead cost is defined as the number of message exchanges. In case of these message exchanges have been either lost or traveling through multihops, the MT will get annoyed and try to issue another request in order to access the FN. When the number of hops increases between the FN and HN, the message delays increase too. In case of communication links never disconnect, there are some obvious components causing delay at each hop (i.e. queueing, transmission, propagation, and waiting time) [13].

In this thesis, a generic scenario is considered when a FN needs to authenticate MTs and the MTs always roam into a FN. If a MT makes a new connection in a subnet of a FN, it calls for session authentication. When the MT moves from the current subnet into a new subnet within the FN, this is known as intra-domain handoff authentication. However, if the MT moves from the current subnet into a new subnet outside the current FN, this is known as inter-domain handoff authentication [14]. Whenever the MT needs to make a new connection or handoff an existing connection, the MT needs to be authenticated.

2.3 Objectives of Designing Authentication Protocols

The necessity of designing robust and efficient authentication protocols is apparent in wireless today's applications. The requirements of authentication protocols can be summarized in the following points:

Security Robustness : It is the main objective in designing security protocols. Authentication protocols should prevent any type of attack such as man-in-the-middle and replay attack. Most, if not all, of authentication protocols consider security robustness as one of the major components during the design.

Power efficiency : Authentication protocols should use less power especially for mobile users which are known to have limited power.

Network efficiency : Authentication schemes should maintain the overhead as low as possible; fast authentication process is preferable in user's points of view.

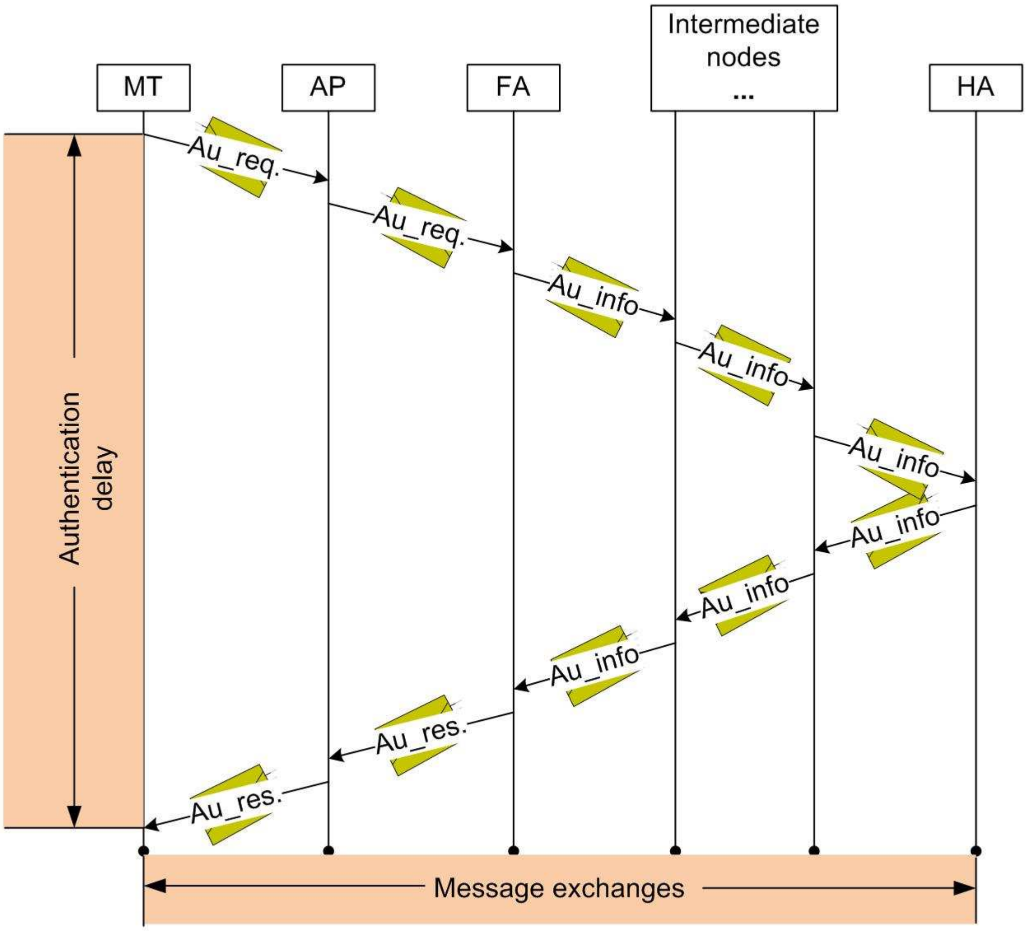

Figure 2.1: Authentication process

Network diversity : For heterogenous networks, authentication schemes should considerate the characteristics of different networks. In particular, Wireless networks are different than wired networks so that authentication protocols should take into account the characteristics of wireless medium.

Chapter 3

Credit-Based User Authentication for Delay Tolerant Networks

WLANs have become very popular due to low cost, easy deployment, and ubiquitous Internet access. The promising of metropolitan Internet access changes the future of networking by meaning of multihop wireless networks. However, enabling Internet access in multihop wireless networks makes Internet more challenging [15], mainly due to the increasing delays. In this chapter, we first provide a general overview of delay tolerant networks in section 3.1. We present the related work in section 3.2, followed by the problem formulation in section 3.3. Finally, the credit-based authentication for delay tolerant networks that have high latency is proposed in section 3.4.

3.1 Delay Tolerant Networks

3.1.1 Background

The success of Internet protocol was based assumedly on the existing end-to-end connection path. If this connection path is intermittent, the Internet protocol stacks are not behave well [16, 17, 18, 19]. The major problem with Internet protocol is transmission control protocol (TCP) . TCP does not work well in high delay networks because TCP requires three-way handshaking to establish a connection and this three-handshaking takes 1.5 round-trip times (RTTs) [16]. In high delay networks, one round-trip may take minutes, hours, or even days. Thus, a TCP connection may not successfully established before timeout. Let's consider some examples:

- The idea of delay tolerant networks was mainly from interplanetary network (IPN) by National Aeronautics and Space Administration (NASA) [17, 18]. NASA's objectives were to make the communication between the Earth and spacecrafts, or remote areas in the Moon, as smooth as the communications between two people in the Earth. The main difficulties of space communication arise high propagation delays and variations of delays.

- In sensor networks, sensor devices are planted on animals to track and protect them. Due to the nature of animals migration, connections between these portable transmitters and the central base station are intermitted. So, intermittent links cause high delay.

3.1.2 Characteristics of Delay Wireless Tolerant Networks

The wireless network is characterized by possible intermittent connectivity and large transmission delays due to user mobility, sparse mobile node distribution, link failures (because of hostile propagation medium), or other high-priority traffic. Although multiple-hop wireless backhaul extends the coverage, such characteristics cause even more performance impact with the deployment of multi-hop wireless backhaul due to transmission failure in any hop resulting in failed end-to-end packet delivery.

For better understanding, it is very important to characterize the DTNs. The main concern in challenged networks is delay. The characteristics of the DTNs can be viewed as communication link characteristics and end system capabilities [19]. It could be described as follows:

Path and Link Characteristics Disconnections of communication links, low data rates, high transmission delays, high propagation delays, node motilities, and/or high error rates in communication media are some forms of DTN characteristics.

End System Capabilities End systems are limited power, bounded memory space, and/or low processing capability. For instance, if end mobile systems have power-life less than connection time occurred.

3.1.3 Solutions

Some solutions have been proposed in the literature in order to adapt the Internet stack to unusual behavior networks. Proxies are an example which are placed on the boundary to deal with these networks. These proxies have either limited scalabilities or wasted resources [19]. Thus, new and back compatible network architecture is needed to manage the behaviors of the challenged networks and to map among different types of networks.

While most multimedia data are loss tolerable, it is a good idea to apply the concept of delay tolerant network (DTN) [19] to the mobile wireless network when delivering integrity sensitive data, such as secure bank transactions, stock information, etc. The DTN was originally designed for multihop interplanetary communications [18], where extreme long transmission delay and high error rate are expected. Generally, the DTN nodes use store and forward technique so that costly end-to-end re-transmission in poor transmission channel can be avoided [19].

Internet Research Task Force (IRTF) created a research group for DTN called Delay-Tolerant Networking Research Group (DTNRG) . This group is concerns how to propose an architectural and protocol design principles arising from the need to provide interoperable communications with and among extreme and performance-challenged environments where continuous end-to-end connectivity cannot be assumed [20]. The DNTRG is developing two main protocols bundle protocol [21] and licklider transmission protocol (LTP) [22] . The difference between LTP and bundle protocol is that LTP is a point-to-point protocol meaning that there are no routing and congestion overhead involved, but bundle protocol is not. Bundle protocol is an overlay protocol to support delay tolerant between application interfaces and transport layer [20, 19]. In Internet stack, bundle protocol places above TCP/UDP protocol.

3.1.4 Integrated all-IP Delay Tolerant Networks

Figure 3.1 shows a generic all IP-based mobile wireless network infrastructure with heterogeneous network connectivity. The wireless front end radio access technologies, denoted as access point (AP) in the figure 3.1, may include cellular mobile networks for large service areas and IEEE802.11/16 for high-rate transmission over service hot spots. Mobile IP (MIP) protocol [23] [24] is applied to support IP mobility for mobile clients. It can be seen in the figure, multiple hop IEEE802.16 backhauls, as well as the satellite link, are key components to greatly extend the Internet service. The service providers include well-know major network carriers and independent vendors. The home networks of those independent vendors may be connected to the IEEE802.16 backhaul, such as HN2 in the figure.

In the future, we are going to face more challenged networks, such networks like interplanetary internet, sensor networks, and deep space communication. It has been shown that Internet protocols do not work well in some challenged networks and a lot of research has been studied the literature [16, 17, 19].

Therefore, the efficiency of packet transportation can be greatly improved without losing delivery guarantee, and the minimum deployment density of wireless backhaul hubs (BHs) can be further reduced.

3.2 Related Works

Much research has been introduced related to single or multi-integrated mobile wireless networks [25, 26, 27, 28, 29, 30]. Integrated wireless networks have been extensively studied

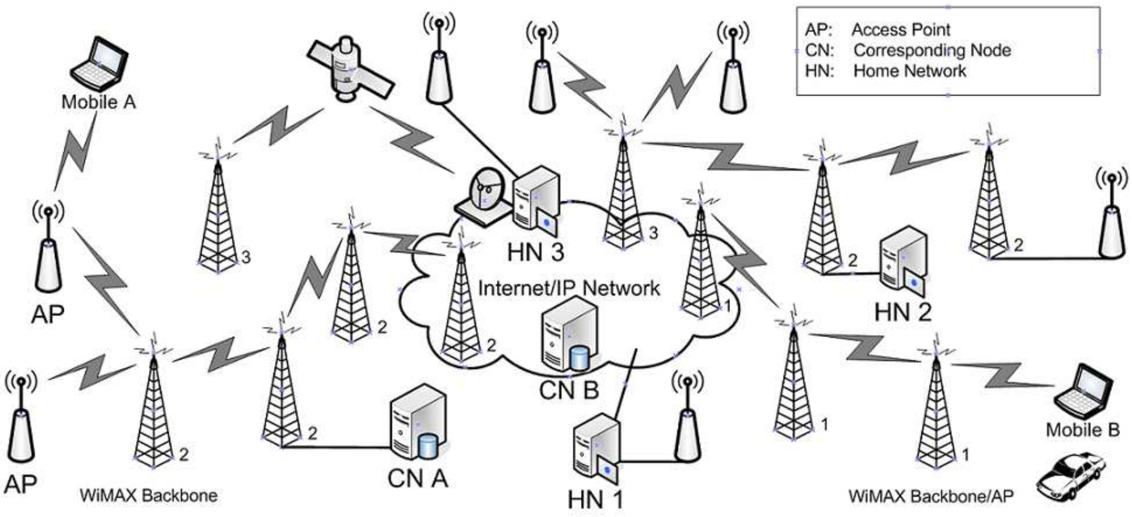

Figure 3.1: Delay tolerant integrated mobile wireless networks

in the literature [25, 26]. In [27], an integration scheme is proposed by active interaction authentication scheme. It can be done through a secured Web page for login over a hypertext transport protocol secured (HTTPS) connection. This scheme does not provide seamless roaming. Other authentication schemes in [28], [29] and [30] are made by localizing at the foreign network (FN) to reduce delay and overhead. However, the cached user credential is stored only in the FA . These schemes do not work properly in challenge networks due to unauthenticated data voyaged.

Authentication affects both security and QoS [31, 32, 33]. Plenty of research works have analyzed authentication systems by the meaning of security robustness. Researchers have analyzed authentication protocols in terms of network performance [34, 35, 14]. They have studied challenge/response authentication based in wireless networks in terms of signaling and processing load of cryptographic techniques.

3.3 Research Objectives

The main objective of the thesis is to propose an authentication scheme for delay tolerant networks, and to analyze and evaluate the scheme in terms of overhead cost and authentication delay. The proposed scheme inherits the idea from our daily life. Credit system has been tightly integrated into our society. It has been proven that credit system works very well and effectively, as seen from the economics system point's view. Typically, credit system takes small risk for greater benefit, considering that most, if not all, members in the society are rational.

3.4 Credit-Based Authentication Architecture

Authentication protocols are the basis of security fundamentals. Based on the authentication protocols, a responder can verify and authority the requester's identity based on the responder's policy. The authentication in networking is that a requester needs to authenticate itself by sending out authenticated information to the attachment's point, responder. The responder responses based on its policy.

In the delay tolerant mobile networks, the major effecting is delay. This delay can be caused by multi-hop wireless backhaul, link failure, or high channel errors. Most authentication protocols are synchronized meaning that the FA can not allow the MT to get access into its network unless the FA receives positive acknowledgement from the HA. As a result, the legitimate mobile user should be able to access the network as soon as possible. Therefore, authentication process should eliminate the effect of the long delay.

In this thesis, the credit-based user authentication for delay tolerant networks is proposed [36]. Authentication credit is created for the mobile terminal when the mobile terminal accesses the network service. Before a mobile terminal accesses the network service of the FN, the FA performs authentication process to check the legitimate of the attempted MT. If the authentication process is positively successful, the FN registers the legitimate MT. Subsequently, if the MT reattempts access the FN, the FA should avoid full authentication due to the good history of the MT. Credit-based system is proposed to speed up the authentication process. In reality, credit system has been emerged in our society and it works very effective. The benefits of the credit-based user authentication reduce the overall overhead, decrease the authentication delay, and allow more users to access. The downside of the credit authentication system is the time, which is called credit time T_i^{credit}, of whether the HA having acknowledged negatively or timeout. Credit system, typically, takes small risk for greater benefit.

The proposed credit authentication process is demonstrated in Figure 3.2. When the MT sends authentication request to the FA through the attachment's point BH or AP, the front end checks whether the MT has an authentication credit (AC) or not. If the MT does not have an AC, the authentication request is forwarded until it reaches the foreign agency (FA). The FA verifies the MT legitimacy with the home agency (HA) with tolerance delay. If the HA responses positively, the FA approves the MT's access request and assigns a credit to the MT and each hub along its path. The authentication delay is expected to be high because it is first verification. If either the HA responses negatively or the tolerance

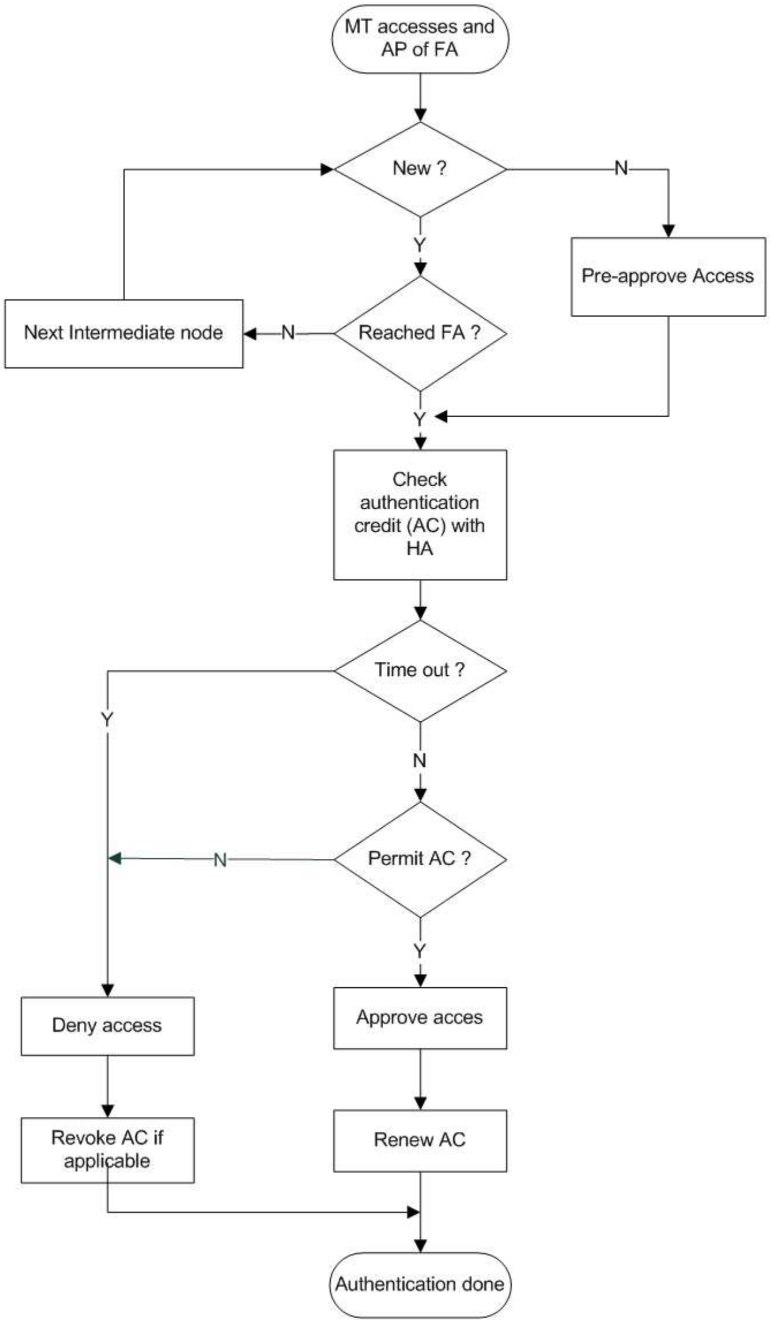

Figure 3.2: Flow chart of proposed credit-based authentication scheme

delay is reached, the access will be denied.

Whenever the MT re-accesses the FN, based on its access location, the MT is allowed to access and at the same time the authentication credit is verified with its HA. A full authentication is performed in the background; therefore, the MT isolates from the possible long delay. When the FA receives a positive acknowledgment, the FA verifies and renews the credit to the MT and each hub along the path. The credit is revoked by either the HA's acknowledgment being negative or the tolerance delay reaching credit time T_i^{credit}. This implies the MT's account standing is not valid.

3.4.1 Authentication Credit

We define the authentication credit $AC_i = ACID_i||\, ID_M||\, ref_i||\, exp_i : Sig_F$, where $ACID_i$ denotes the identity of the authentication credit assigned by the FA, ref_i denotes the authentication credit reference code, and exp_i denotes the authentication credit expiration time. The FA stores the mapping $AC_i \longleftrightarrow ID_H \longleftrightarrow k_i$ in its database after it receives positive verification of the MT from the HA. A parameter called pre-approval timeout T_i^{credit} is defined based on the expected time to receive the response from the HA and is used in the visited network internally. This parameter defines the absolute time when the authentication credit is expired so that both the MT and FA do not keep the credit forever.

Chapter 4

Performance Analysis of Credit-Based Authentication Scheme

This chapter presents an analytical model for evaluating the authentication scheme and estimating a proper credit time (T_i^{credit}) for each wireless network i. The cost is defined as the overhead message exchanges in the overall network. Delay is defined as the time elapsed of sending a packet from a source to a destination. This chapter is divided into two parts. The cost analysis is presented in Section 4.1. Secondly, the delay model is introduced in Section 4.2.

4.1 Cost Analysis

We assume that there are N hotspot networks so that the mobile user may show up to any one of them at anytime. The mobility pattern of the MT is based on the residence time which is assumed to be exponentially distributed random variables with rate ξ_i ($i = 1, 2, \ldots, N$).

Let $\Phi(t)$ denotes a process that tracks the MT at which network is connected at the time t. Therefore, the process $\Phi(t)$ can be modeled as a continuous markov process, as shown in Figure 4.1. By sampling the random process $\Phi(t)$ after time instances $t_k = k * \delta$, where $\delta < (max_i \xi_i)^{-1}$ $\forall i$, the new sampled process $\Phi(t_k)$ is a markov chain [37], in the state space $S = \{WLAN_1, WLAN_2, \ldots, WLAN_N\}$, defined by the transition probability matrix

$$P = \begin{bmatrix} 1 - p_1 & p_1 * q_{12} & p_1 * q_{13} & \ldots & p_1 * q_{1N} \\ p_2 * q_{21} & 1 - p_2 & p_2 * q_{23} & \ldots & p_2 * q_{2N} \\ p_3 * q_{31} & p_3 * q_{32} & 1 - p_3 & \ldots & p_3 * q_{3N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_N * q_{N1} & p_N * q_{N2} & p_N * q_{N3} & \ldots & 1 - p_N \end{bmatrix}, \tag{4.1}$$

where $p_i = 1 - e^{-\xi_i \delta}$ for $i = 1, 2, \ldots, N$. q_{ij} is the roaming probability from the $WLAN_i$ to $WLAN_j$. It can be represented the roaming probability as the following matrix

$$Q = \begin{bmatrix} 0 & q_{12} & q_{13} & \ldots & q_{1n} \\ q_{21} & 0 & q_{23} & \ldots & q_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ q_{n1} & q_{n2} & q_{n3} & \ldots & 0 \end{bmatrix}, \tag{4.2}$$

and $\sum_{i=1}^{N} q_{i,j} = 1$. Q matrix is to distinguish access probability from $WLAN_i$ to $WLAN_j$ for $\forall i, j \in S$.

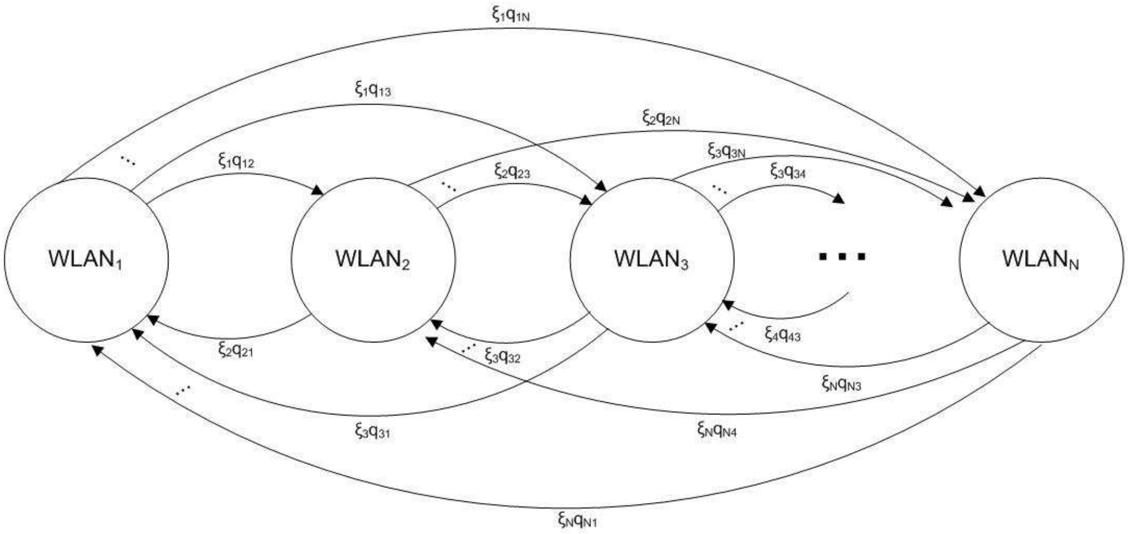

Figure 4.1: Mobile user roaming

4.1.1 Average Overhead Cost

We are interested in defining the overhead cost as the cost-function. The overhead cost C is defined as the average authentication message exchanges requiring real-time transactions per network switching and can be computed by

$$C = \sum_{i=1}^{N} \pi_i C_i, \tag{4.3}$$

where π_i is the long-run proportion of time that the process will be in state i and C_i is equal to $Pr_i\{\text{credit exit}\}C_i^{credit} + (1 - Pr_i\{\text{credit exit}\})C_i^{no\_credit}$, where C_i^{credit} and $C_i^{no\_credit}$ are average overhead costs in roaming to wireless network i with stored authentication credit, and wireless network i without stored authentication credit, respectively. $Pr_i\{\text{credit exit}\}$ is the probability that the MT revisits the wireless network i before the credit expired, i.e., the MT revisits within the time interval k. If k is equal to zero, full authentication is needed. Otherwise, full authentication is performed in the background. $Pr_i\{\text{credit exit}\}$ can be computed by

$$Pr_i\{\text{credit exit}\} = \sum_{j=1}^{N} \alpha_j * Z_{ji}^{k}. \tag{4.4}$$

α is defined as a vector (e.g. $\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_N]$), where α_j is the initial probability that the MT is in $WALN_j$, k is equal to $\lfloor \frac{t_i^{credit\_expired}}{\delta} \rfloor$, and $\mathbf{Z}$ matrix can be obtained by replacing i^{th} row of matrix $\mathbf{P}$ by its identity matrix.

4.1.2 Average Credit Time

We are interested in estimating the credit time for long term. It can be defined as the average time that the MT gets credit time and can be computed by

$$C_t = \sum_{i=1}^{N} \pi_i T_i^c, \tag{4.5}$$

where π_i is the long-run proportion of time that the process will be in state i and T_i^c is equal to Pr_i\{credit exits\} T_i^{credit}. Denoting that T_i^{credit} is the credit time and Pr_i\{credit exits\} is the probability of revisiting $WLAN_i$ before the ticket, T_i^{credit}, is expired.

4.2 Delay Analysis

We consider independent wireless networks and they are partially connected, but there is always a path from any source to any destination based on a routing algorithm R. When a mobile node roams to a new area, it needs to be authenticated by a new foreign agent (FA).

A packet delay of one-round trip from a source to a destination can be modeled as a chain network based on a routing algorithm R [13]

$$D = \sum_{i \in R} T_i, \tag{4.6}$$

where T_i is the packet time duration at each hop i towards to its destination. We use M/G/1 queuing model for each node. The service time is the time when a packet arrives at the next hop successfully followed by its acknowledgement including retransmission the packet when corrupted packet occurs. M/G/1 uses first come first served (FCFS) scheduling scheme.

Each hop h has Poisson arrival at rate λ_h, and a general service distribution is denoted as μ_h of single channel. We do not consider the processing delay at each hop. The average waiting time in the queue at hop h can be computed according to Pollaczek-Khintchine (p-k) formula [38]

$$\overline{W}_h = \frac{\lambda_h \overline{X_h^2}}{2(1-\rho_h)} \tag{4.7}$$

$$W_h^*(s) = \frac{s(1-\rho_h)}{s-\lambda+\lambda G^*(s)}, \tag{4.8}$$

where $\overline{X}_h = \frac{1}{\mu_h}$ is the average service time, $\overline{X_h^2}$ is the second moment of the service time, and $\rho_h = \frac{\lambda_h}{\mu_h}$ is utilization factor. $W_h^*(s)$ is the Laplace transform of the queuing waiting time distribution respect to $W^*(s) = \int_0^\infty e^{-sy} dW(y)$. The total time that a packet spent in hop h is

$$\overline{T_h} = \overline{W}_h + \overline{X_h} \tag{4.9}$$

$$T_h^*(s) = W_h^*(s) G_h^*(s), \tag{4.10}$$

where $G_h^*(s)$ is the Laplace transform of the service time distribution and $T_h^*(s)$ is the Laplace transform of the distribution of the total time spent at hop h. The average packet delay from a source to a destination is

$$\overline{D} = \sum_{i \in R} \overline{T}_i \tag{4.11}$$

$$D^*(s) = \prod_{i \in R} T_i^*(s), \tag{4.12}$$

where $D^*(s)$ is the Laplace distribution of one roundtrip time. The summation of the random variable T_i over i is the convolution.

4.2.1 Average Authentication Delay

The performance metric of interest is to study the average authentication delay when a roaming mobile user wanders and sends an authentication request to any FA. The FA does the authentication process to admit this mobile user by contacting HA. Therefore, the integration among wireless service providers is easier and more seamless.

The reason of choosing authentication delay is that MT can not send or receive during this time. If the MT needs to hand off to a new FA, the FA needs to authenticate the MT before handing off. When the authentication delay is high, it will cut off the ongoing connection during handoff, which bothers the MT.

In this thesis, we define the authentication delay as the time that a mobile node sends authentication request until it receives authentication reply. So, the authentication delay can be divided into the time for authentication request ($MT \rightarrow FA \rightarrow \cdots \rightarrow HA$) and the time for authentication replay ($HA \rightarrow \cdots \rightarrow FA \rightarrow MT$). Then, the average authentication request is the summation of the average time needed at each hop from the MT to the HA, and the average authentication response is the summation of the average time takes at each hop from HA to the MT.

Thus, the average authentication delay $\overline{A}$ is the average authentication request plus average authentication response. We assume that the route of the authentication request is the same as the authentication response passing the same number of hops. First, the average authentication request delay is equal to $\overline{T}_M + \sum_{i=1}^{h+1} \overline{T_i}$, where $\overline{T}_M$ is the average service time of MT to send authentication packet to FA. Since MT does not have packets in its queue except authentication request packet, $\overline{T}_M$ is equal to $\overline{X}_M$. Second, $\sum_{i=1}^{h+1} \overline{T_i} + \overline{T}_F$ is the average authentication response delay where $\overline{T}_F$ is the average time to send authentication response from FA to MT. If T_i is independent identically distributed random variable for all nodes including mobile nodes, the average authentication delay is

$$\overline{A} = \overline{T}_M + 2(H+1)\overline{T}_i + \overline{T}_F, \tag{4.13}$$

where H is the average number of hops.

4.2.2 Distribution of Authentication Delay

We are interested in finding the distribution of average authentication delay $P(A > d)$. Using central limit theorem [39], distribution of average authentication delay tends to the normal distribution as $h \to \infty$. Since A_d is the sum of iid variable T_i, A has mean $(2h+4)\overline{X}$ and standard deviation $\sqrt{(2h+4)\sigma}$.

$$Q_A(d) = \frac{1}{\sqrt{(2\pi)(2h+4)\sigma^2}} \int_d^\infty e^{\frac{(A-(2h+4)\overline{x})^2}{2\sigma^2}} dA. \tag{4.14}$$

$Q_A(d) = P(A > d)$ is the Q-function of the authentication delay that the probability of the authentication delay excesses d. Intuitively, when d is large enough, $Q_A(d)$ tends to zero. $Q_A(d)$ is important since it indicates how much time should be given to a roaming user in order not to maintain the connection until the approval comes. If the pre-approval time is too short, it will cause unfavorable connection cutoff. However, very long pre-approval time will be unreasonable since pre-approval time is not paid off.

Chapter 5

Simulation Results

In this chapter, we evaluate the performance of credit-based user authentication scheme in terms of the overhead cost and delay. The overhead of real time transactions (message exchanges) is presented in section 5.1 . Since authentication information is delay sensitive, it is very important to speed up the authentication process. Authentication delay of the proposed model is given in section 5.2. Moreover, the estimation for credit time T_i^{credit} is given in section 5.3. The credit time is the pre-approval time until these connections are approved otherwise they will be blocked.

5.1 Cost Evaluation

The overhead cost function is defined according to Equation 4.3 . It includes the average authentication message exchanges involving real time transaction per MT at each wireless network. Table 5.1 gives the parameters that are used for both analytical and simulation.

Table 5.1: Parameters for Simulation Results

Parameter	Values
Mean residence times $(1/\xi_1, 1/\xi_2)$	$(1/\xi)$ slots
Number of service providers in $WLAN_1$ (Agreement Networks)	10
Number of service providers in $WLAN_2$ (Independent Networks)	20
Sampling time interval	$\delta = 1/(2\xi)$ slot
WLAN 1 and 2 hotsopts average roaming overhead cost with/without cached credentials $\{C_i^{ticket}/C_i^{no_ticket}\}$	(2/4, 2/4) hops
Credit time $(T_1^{credit}, T_2^{credit})$	(0, 300) slots
Packet arrival rate λ at each hop	50 packets/slot
Number of hops H	5

We assume mobility is uniformly distributed.

As stated early, one of the objectives in designing authentication schemes is to reduce the overhead. Figure 5.1 shows that the overhead cost reduces when credit-based user authentication is employed for different values of residence times of the MT. As the residence time decreases, the overhead decreases. When the MT is legitimate, the AC renewal process reduces the authentication overhead effectively. In order to validate our analytical model, a C++ program simulation is developed [40] [41]. As shown in Figure 5.1, the simulation results match the analytical results well.

As mention in Section 4.1.2, the service providers would like to know how much unprofitable time is given to the mobile users. Our calculation using Equation 4.5 gives the average time credit. Figure 5.2 shows average time credit versus authentication credit expiration for different values of residence times of the MT. As the credit time expiration increases, the unprofitable time increases. As shown in the figure, the simulation results

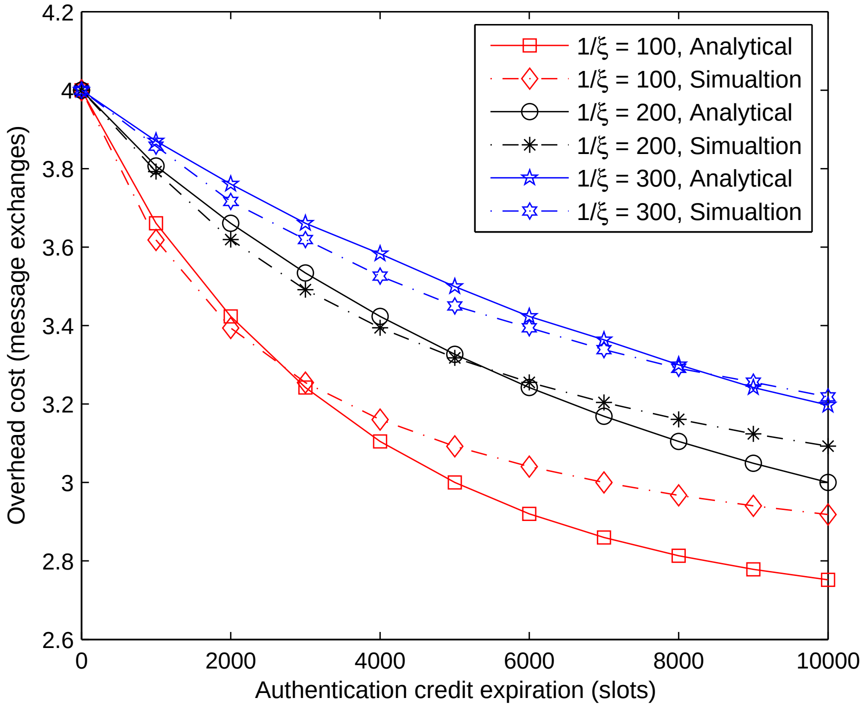

Figure 5.1: Overhead cost vs. authentication credit expiration

match the analytical results well.

From Figures 5.1 and 5.2, there is a tradoff between the overhead and credit time. Choosing the authentication credit expiration is important, and finding the optimal value for the authentication credit expiration is our future research direction.

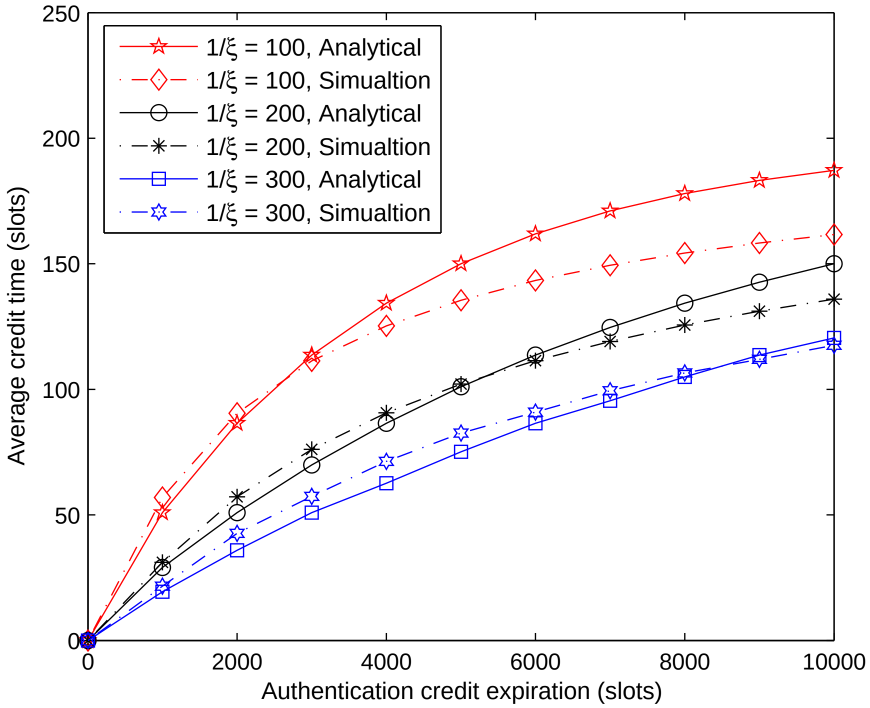

Figure 5.2: Average authentication time vs. authentication credit expiration

5.2 Delay Evaluation

We are interested in how long authentication process will take. We assume the packet arrival rate at each hop is given by $\lambda = 50$ packets/slots, while the packet service rate of

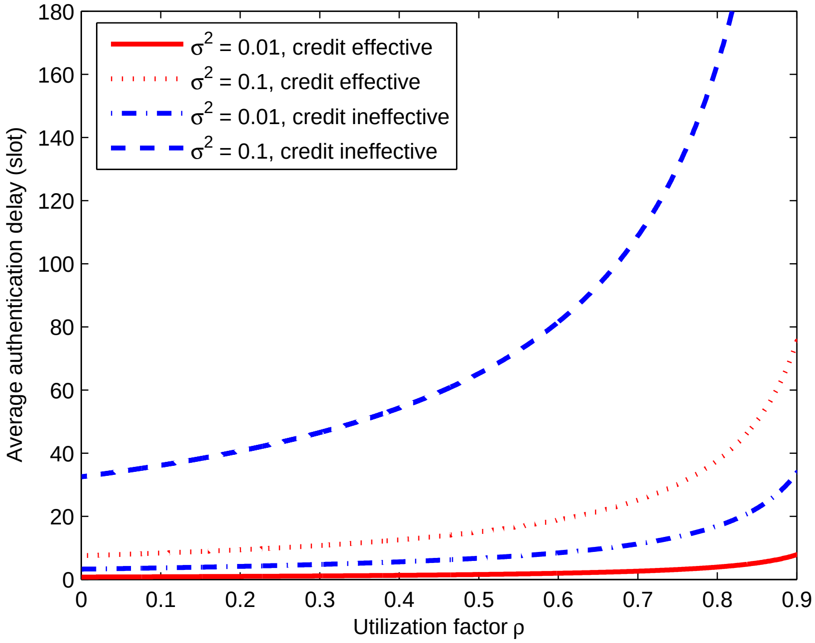

Figure 5.3: Average authentication delay vs. service utilization factor

each hop is variable and denoted by packets/slot. The packet service time can be described as the time for transmitting a packet correctly to the next hop towards to its destination. Figure 5.3 shows the average authentication delay vs. service utilization factor per hop with different wireless channel variance σ with different authentication types when Table 5.1 is used. As the channel variance increases, the average authentication delay increases as well dramatically. It can be observed that the proposed authentication scheme could significantly reduce the authentication latency in the delay tolerant wireless network where the channel condition is usually not good or the connection is intermitted. We assume the call admission control is employed at each hop so that no traffic density is more than

$\rho = 0.9$ as shown in the Figure 5.3.

5.3 Estimating Credit Time T_i^{credit}

In implementing pre-approval mechanism, it is important to set pre-authentication timeout properly since it is not profitable to set the timeout unnecessary too long, and too short setting will cause annoying network connection cutoff. Figure 5.4 shows the probability of authentication time versus the time line for different wireless channel condition. We assume 90% utilization factor. It can be seen that the background authentication time varies based on the wireless channel condition. The background authentication process at poor channel condition $\sigma^2 = 0.2$ needs up to almost twice as long as the one at good channel condition $\sigma^2 = 0.0$. Therefore, the result obtained from the figure can be used for estimating proper setting for the credit time T_i^{credit}.

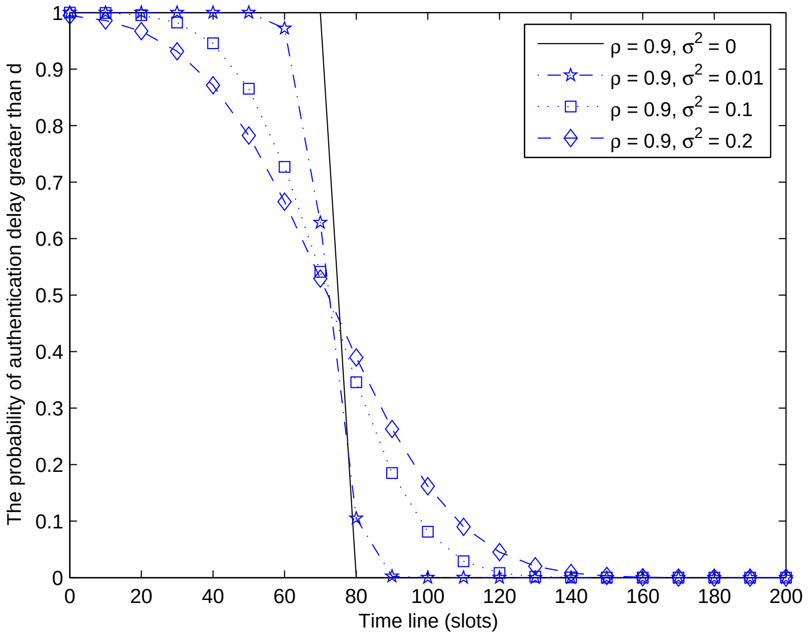

Figure 5.4: Probability of the authentication delay distribution

Chapter 6

Conclusion and Future Works

6.1 Conclusion

In this thesis, a credit-based user authentication scheme has been presented for delay tolerant mobile wireless networks. The proposed authentication scheme adopts renewable authentication credit and multi-point localized authentication mechanisms to isolate the user authentication process from uncertain network condition in the wireless backhaul. A mobile user is very likely to be able to access the network resource without excess waiting in the visited network. The performance evaluation has been provided to demonstrate that the proposed credit-based authentication scheme is secure and effectively reduces the overall delay and overhead in user authentication for delay tolerant mobile wireless networks.

6.2 Future Works

Although the proposed credit-based user authentication scheme is mainly designed for delay tolerant mobile wireless networks, this scheme can be applied to delay and loss tolerant networks, or the Internet. However, The major difference is the credit time T_i^{credit}. Thus, adapting model for estimating the credit time is an important aspect. For example, the credit time for wired Internet should not be the same as that for the wireless Internet, in other words, the credit time for wired Internet is very less than for the wireless Internet .

Since the authentication credit is distributed, we should avoid comprised authentication credit. Moreover, this authentication credit can be more helpful in the sense that authenticated data can be routed through hops and those hops can build a credit history for this mobile user and its home network.

Our credit system can be based on authenticated or not authenticated history. The credit system can exploit more than ”Yes” or ”No” history. It can track the mobile users' activities and/or its home network for further security and/or billing proposes. Moreover, the authentication credit could be used as an identification (ID) and hides the real identity of the mobile user.

There are some other issues related to delay tolerant networks: security and routing. Security has been an open issue, so there are still some security issues that need to be considered in DTNs [42, 43]. For example, denial of service (DoS) attacks is very serious. To resolve DoS attacks, randomized ID could be used. Routing in delay tolerant networks is different than other networks because of the mobility and/or link disconnection [44].

Bibliography

[1] IEEE standard 802.11b supplement. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Higher-speed physical layer in the 2.4 GHz band, August 1999.

[2] IEEE standard 802.11a supplement. Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications. High-speed physical layer in the 5 GHz band, July 1999.

[3] IEEE 802.16-2004. IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, 2004.

[4] C. Eklund, R.B. Marks, K.L. Stanwood, and S. Wang. IEEE standard 802.16: a technical overview of the WirelessMAN air interface for broadband wireless access. *Communications Magazine, IEEE*, 40(6):98–107, Jun 2002.

[5] M. Leech. Username/Password Authentication for SOCKS V5. *RFC9129*, March 1996.

[6] C.E. Perkins and P.R. Calhoun. Mobile IP Challenge/Response Extensions. *draft-ietfmobileip-challenge-09.txt*, February 2000.

[7] W. Simpson. PPP Challenge Handshake Authentication Protocol (CHAP). *RFC1334*, August 1996.

[8] IEEE standard 802.11. Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications, August 1999.

[9] N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: the insecurity of 802.11. In *MobiCom '01: Proceedings of the 7th annual international conference on Mobile computing and networking*, 2001.

[10] W. A. Arbaugh, N. Shankar, and Y.C. Wan. Your 802.11 wireless network has no clothes. *Wireless Communications, IEEE*, 9(1):44–51, 2002.

[11] W. Stallings. *Network Security Essentials*. Prentice Hall, 2nd edition edition, 2002.

[12] http://www.certicom.com. Certicom corp., 2007.

[13] D. P. Bertsekas and R. G. Gallager. *Data networks*. Prentice Hall, Englewood Cliffs, N.J., 2nd edition, 1992.

[14] W. Liang and W. Wang. On performance analysis of challenge/response based authentication in wireless networks. *Computer Networks,*, 48(2):267–288, 6/6 2005.

[15] K. Xu, S. Bae, S. Lee, and M. Gerla. TCP behavior across multihop wireless networks and the wired internet. In *WOWMOM '02: Proceedings of the 5th ACM international workshop on Wireless mobile multimedia*, pages 41–48. ACM Press, 2002.

[16] S. Farrell, V. Cahill, D. Geraghty, I. Humphreys, and P. McDonald. When TCP Breaks: Delay- and Disruption- Tolerant Networking. *Internet Computing, IEEE*, 10(4):72–78, 2006.

[17] S. Burleigh, A. Hooke, L. Torgerson, K. Fall, V. Cerf, B. Durst, K. Scott, and H. Weiss. Delay-tolerant networking: an approach to interplanetary Internet. *Communications Magazine, IEEE*, 41(6):128–136, 2003.

[18] Consultative Committee for Space Data Systems (CCSDS). www.ccsds.org, 2007.

[19] K. Fall. A Delay-tolerant Network Architecture for Challenged Internets. In *SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 27–34, New York, NY, USA, 2003. ACM.

[20] Delay-Tolerant Networking Research Group (DTNRG). http://www.dtnrg.org/, 2007.

[21] K. Scott and S. Burleigh. Bundle Protocol Specification. 2007.

[22] M. Ramadas, S. Burleigh, and S. Farrell. Licklider Transmission Protocol - Specification. 2007.

[23] C. Perkins. IP Mobility Support for IPv4. 2002.

[24] C. Perkins and D. Johnson. Mobility support in IPv6. In *MobiCom '96: Proceedings of the 2nd annual international conference on Mobile computing and networking*, pages 27–37, New York, NY, USA, 1996. ACM.

[25] A. Alkassar and C. Stuble. Security framework for integrated networks. *Military Communications Conference, 2003. MILCOM 2003. IEEE*, 2003.

[26] W. Wang, W. Liang, and A. Agarwal. Integration of authentication and mobility management in third generation and WLAN data networks. *Wirel. Commun. Mob. Comput.*, 5(6):665–678, 2005.

[27] M. M. Buddhikot, G. Chandranmenon, S. Han, Y.-W. Lee, S. Miller, and L. Salgarelli. Design and implementation of a WLAN/cdma2000 interworking architecture. *Communications Magazine, IEEE*, 41(11):90–100, 2003.

[28] M. Shi, H. Rutagemwa, X. Shen, J. W. Mark and A. Saleh. A Service-Agent-Based Roaming Architecture for WLAN/Cellular Integrated Networks. *Vehicular Technology, IEEE Transactions on*, 56(5):3168–3181, 2007.

[29] M. Long, C.-H. Wu, and J.D. Irwin. Localized authentication for wireless lan internetworking roaming. *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, 1:264–267 Vol.1, 21-25 March 2004.

[30] X. Lin, H. Zhu, P.-H. Ho and X. Shen. Two-Factor Localized Authentication Scheme for WLAN Roaming. In *Communications, 2007. ICC '07. IEEE International Conference on*, pages 1172–1178, 2007.

[31] N.A. El-Fishway, M.A. Nofal, and A.M. Tadros. An improvement on secure communication in PCS. *Performance, Computing, and Communications Conference, 2003. Conference Proceedings of the 2003 IEEE International*, pages 175–182, 9-11 April 2003.

[32] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, and S. Miller. Efficient authentication and key distribution in wireless IP networks. *Wireless Communications, IEEE*, 10(6):52–61, Dec. 2003.

[33] Y.-M. Tseng, C.-C. Yang, and J.-H. Su. An efficient authentication protocol for integrating WLAN and cellular networks. *Advanced Communication Technology, 2004. The 6th International Conference on*, 1:416–420, 2004.

[34] W. Liang and W. Wang. An analytical study on the impact of authentication in wireless local area network. In *Computer Communications and Networks, 2004. ICCCN 2004. Proceedings. 13th International Conference on*, pages 361–366, 2004.

[35] W. Liang and W. Wang. A quantitative study of authentication and QoS in wireless IP networks. *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, 2:1478–1489 vol. 2, 13-17 March 2005.

[36] M. Shi, K. Almotairi, X. Shen, J.W. Mark, and D. Zhao. Credit-Based User Authentication for Delay Tolerant Mobile Wireless Networks. *Proc. IEEE ICC'08, Beijing, China, May 19-23, 2008.*

[37] R. G. Gallager. *Discrete stochastic processes.* The Kluwer international series in engineering and computer science. Kluwer, Boston, 1996.

[38] L. Kleinrock. *Queueing systems, Vol. 1.* Wiley, 1975.

[39] M. R. Sheldon. *Introduction to probability models.* Academic Press, Amsterdam, 2003.

[40] B. Stroustrup. *The C++ Programming Language.* Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2000.

[41] A. M. Law and W. D. Kelton. *Simulation modeling and analysis.* McGraw-Hill series in industrial engineering and management science. McGraw-Hill, New York, 2nd edition, 1991 1990.

[42] S. Farrell and V. Cahill. Security Considerations in Space and Delay Tolerant Networks. In *SMC-IT '06: Proceedings of the 2nd IEEE International Conference on Space Mission Challenges for Information Technology*, pages 29–38, Washington, DC, USA, 2006. IEEE Computer Society.

[43] A. Seth and S. Keshav. Practical security for disconnected nodes. *Secure Network Protocols, 2005. (NPSec). 1st IEEE ICNP Workshop on*, 6 Nov. 2005.

[44] S. Jain, K. Fall, and R. Patra. Routing in a delay tolerant network. In *SIGCOMM '04: Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 145–158, New York, NY, USA, 2004. ACM.