A Local Authentication Control Scheme Based on AAA Architecture in Wireless Networks

Wei Liang
Department of Electrical and Computer Engineering
North Carolina State University
Raleigh, North Carolina 27695–7911
Email: wliang@eos.ncsu.edu

Wenye Wang
Department of Electrical and Computer Engineering
North Carolina State University
Raleigh, North Carolina 27695–7911
Email: wwang@eos.ncsu.edu

***Abstract*— In this paper, we propose a novel control scheme to locally authorize inter-domain roaming users for efficient authentication in wireless networks, which is based on authentication, authorization, accounting (AAA) architecture. We develop a detailed procedure to establish local security associations (SAs) for authentication and determine a threshold to trigger the proposed scheme. By considering the traffic and mobility patterns of a mobile user (MU), as well as the number of hops between the MU and its home AAA server, we demonstrate that the performance of the proposed scheme outperforms DIAMETER protocol with respect to authentication latency and cost for macro-mobility users with a high volume of authentication requests.**

I. Introduction

In wireless networks, security and quality of service (QoS) are both important in providing reliable communications because of the unprotected and bursty open medium. To provide security services in wireless networks, authentication is a process to identify mobile users (MUs) and negotiate credentials such as keys and algorithms for secure communication [1].

When an authentication process is initiated, an authenticator requires an MU to submit credentials such as certificates and challenge/response values for verification. The verification is performed with a security association (SA), which is a relationship that affords security services with parameters such as session keys between the MU and its authenticator. With the confidential verification, the authentication can protect authorized access to network resource for legitimate users. The information secrecy and data integrity can also be guaranteed by using the negotiated secret credentials for encryption and message authentication.

Meanwhile, the authentication process has a great effect on the QoS such as authentication latency and cost due to additional overheads [2], [3]. When public/private-key based authentication mechanism is applied, the computation complexity consumes much time and power [2]. On the other hand, in secret-key-based authentication, due to the lack of SA between the roaming MU and the foreign authenticator, the credentials of the MU are encrypted hop-by-hop and transmitted back to its home network, which may cause higher authentication cost in terms of signaling and encryption/decryption, and long authentication delay [4], [5].

In order to reduce authentication cost, an authentication, authorization and accounting (AAA) architecture is proposed for wireless networks [6]. In this architecture, an AAA server is a central server in one autonomous network with hop-by-hop SAs between AAA servers for authentication. Based on this architecture, the credentials are delivered from a local AAA server (LAS) to the home authentication server (HAS) for authentication when the MU is roaming in foreign networks, regardless of the traffic and mobility patterns of the MU as well as the distance between the MU and its HAS. These operations deteriorate the QoS with expensive authentication cost and long latency, especially for two networks far from each other [3], [4], [6], [7]. In addition, remote authentication imposes heavy cost burden on servers because hop-by-hop encryption/decryption is applied due to the lack of a direct SA in the AAA architecture.

In this paper, we first propose a local authentication protocol, which is able to securely establish a local SA for inter-domain roaming MUs and produce challenge/response values for local authentication. Second, we consider the mobility and traffic patterns to determine a threshold for triggering the proposed scheme. With this scheme, we not only reduce the authentication delay and cost significantly, but also provide a framework to account for the traffic and mobility patterns in authentication efficiency, as well as feasible implementation in any wireless networks using the AAA architecture.

The rest of this paper is organized as follows. In Section II, we introduce the concepts of SA, AAA architecture, and challenge/response authentication mechanism. Based on the application of these concepts, we propose a local authentication control scheme in Section III. We evaluate and show the advantage of proposed scheme in terms of authentication cost and delay by comparing to DIAMETER protocol in Section IV. Finally, we draw a conclusion in Section V.

II. Overview of Authentication on AAA Architecture

In this section, we introduce the authentication on AAA architecture, with the concepts of security association, challenge/response authentication, and AAA architecture.

0-7803-8521-7/04/$20.00 © 2004 IEEE

A. Security Association

As defined in IP security architecture (IPsec), security association (SA) is a trust relationship between a sender and a receiver that affords security services to the traffic. It has many parameters, such as security parameters index (SPI), key and lifetime, all of which can be used to serve for encryption and authentication [8]. An SA can be established and modified with protocols such as Internet security association and key management protocol (ISAKMP), secure socket layer (SSL) or transport layer security (TLS). In these protocols, SSL and TLS are two protocols commonly used in mobile networks. SSL is a standard for encrypted client/server communication between network devices. It works by using a public key to encrypt and transfer data. TLS is an IETF standard with the goal to produce an Internet standard version of SSL [9]. However, all of the algorithms applied in this protocol are time-consuming, especially when the client is an MU with limited calculation capability [2]. The extended authentication time affects many QoS parameters such as packet delay and call dropping probability.

B. Challenge/Response Authentication

In order to facilitate the authentication in mobile networks, secret key based authentication is widely adopted [10]. In particular, challenge/response authentication requires the roaming MU to submit a response value for authentication *each time*, which is encrypted from a *challenge value*, a random value, with an SA shared between the MU and its home network. The challenge and response values are delivered to the home network of the MU for verification. An authentication approval message will be returned if the authentication is granted. However, when an MU initiates a service request or crosses the boundaries of subnetworks, authentication will be triggered. Thus, frequent authentication requests impose a great burden to deliver the authentication messages between networks, which are related with the mobility and traffic patterns of MUs.

Therefore, we propose a local authentication control scheme to establish a local SA and avoid remote authentication with the consideration of mobility and traffic patterns of the roaming MU. The protocol is based on the AAA architecture introduced as follows.

C. AAA Architecture

In order to deliver the authentication messages between networks, many authentication architectures are proposed for different types of mobile networks [6], [11]. In our paper, we consider the authentication, authorization, and accounting (AAA) architecture, which is initially proposed by IETF for Mobile IP networks and is being deployed in 3G systems.

An AAA architecture is composed of local AAA servers (LASs), home AAA servers (HASs), and proxy AAA servers (PASs). An LAS is an AAA server that serves for the visiting MUs in a network domain for AAA functions. An HAS is an AAA server in a network domain that only serves for the MUs who subscribe services in the network domain. A PAS is an AAA server that takes charge of relaying the AAA messages

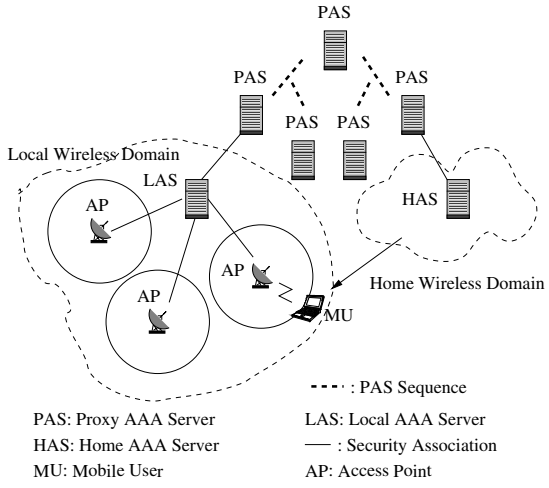

Fig. 1. AAA Architecture in Mobile Networks.

between different AAA servers. All of these AAA servers are organized hierarchically with shared SAs between the AAA server in lower layer and the AAA server in higher layer as is shown in Fig. 1. If the distance between the LAS and the HAS is long, the authentication efficiency in terms of signaling cost and encryption/decryption cost for authentication should be considered. Therefore, some methods are proposed to distribute a permanent local SA for the visiting MU in the local mobile network [5]. However, they do not account for the mobility and traffic patterns of the MU. Furthermore, the permanent life time of the SA will induce the risk of being hacked, which compromises the network security.

To consider the efficiency and security with different mobility and traffic patterns, we propose a local authentication control scheme with local SA control, which can be implemented based on the AAA architecture. Therefore, it can be applied in various mobile environments including 3G, such as CDMA-2000 and UMTS, and 802.11 networks because AAA architecture has been deployed in these networks.

III. Local Authentication Control Scheme

We propose a local authentication control scheme in this section. First, we present an overview of the control scheme. Then, two critical parts of the scheme are introduced. One is the establishment of local SA; the other is to determine the optimal lifetime for the local SA and minimize the authentication cost, which also decreases the latency.

A. Overview of Local Authentication Control Scheme

The framework of the proposed scheme is illustrated in Fig. 2. When an inter-domain authentication request from a visiting MU comes to the LAS, the LAS first checks if a local SA exists for the MU. If the local SA exists, the LAS authenticates the roaming MU with this SA. Otherwise, the LAS checks if the the residence time of the MU will be greater than a threshold value. There are many methods to estimate the residence time of an MU [12]. In our paper, we assume that the estimation result of the residence time exists. Then, if the residence time of the MU is greater than a threshold value, the

LAS will authenticate the MU through the AAA architecture and generate a local SA for it. Otherwise, the LAS simply

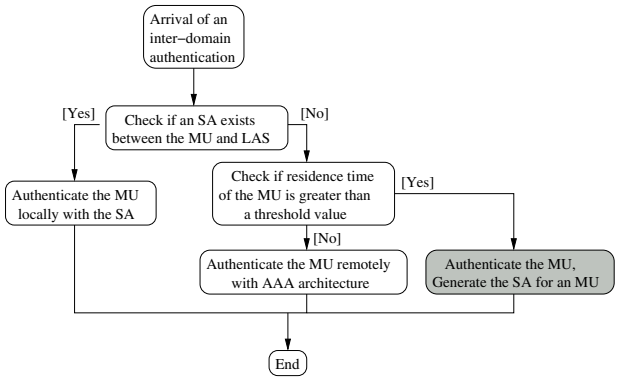

Fig. 2. Overview of Local Authentication Control Scheme.

authenticates the MU though the AAA architecture and does not generate a local SA for it.

If a local SA is generated, we assign the value of residence time of the MU to the life time of the SA. The sequential authentication requests that will arrive within the life time of the local SA can be processed efficiently with the local SA without transmitting the credentials to the HAS of the MU. We focus on the establishment of the local SA in a mobile network for the roaming MU, which is highlighted in Fig. 2. The establishment of a local SA involves with two problems. One is how to distribute the key securely and efficiently; the other is how to determine the threshold value of residence time, i.e., the lifetime of an local SA, which is used to trigger proposed scheme.

B. Authentication and Local SA Establishment Protocol

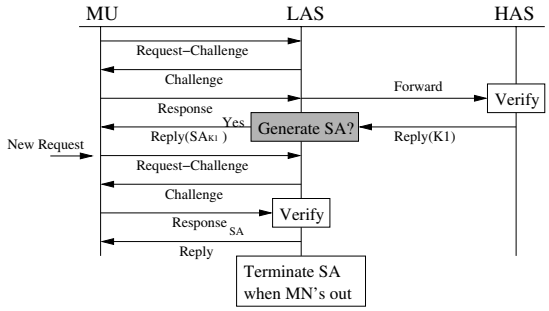

Fig. 3. Authentication and Local SA Establishment Protocol.

The signaling diagram of the protocol to authenticate a roaming MU and establish a local SA for sequential authentication requests is shown in Fig. 3. As we can see in this diagram, when a foreign MU is requesting services in the local network, an authentication request is sent out to the LAS. The LAS replies a challenge, i.e., a random value, to the MU. The MU encrypts the challenge value with an SA shared with the HAS. The result of the value is a response value that is returned to the LAS. Because the LAS has no SA shared with the MU, the LAS relays the response value to the HAS of the roaming MU through the AAA architecture. The HAS of the MU decrypts the response value and compares the result with the challenge value transfered by the LAS. If these two values are matched, the MU is authenticated. A key K_{u1} is generated with the SA shared between the MU and its HAS as follows:

$$K_{u1} = HMAC - MD5(K_0, \{R_1 \| ID_{MU}\}), \quad (1)$$

where K_0 is the pre-shared key in the SA between the MU and its HAS, R_1 is a random value of at least 64 bits. ID_{MU} is the MU's identity. $HMAC - MD5$ is a hash function implemented with MD5. The symbol $\|$ means that the two values are linked together. Then, the message that includes the following data is sent to the LAS:

$$\{K_{u1}, ALGORITHM, F_0, F_i, \{R_1, ALGORITHM, F_0\}_{K_0}\}_{K_i}, \quad (2)$$

where K_{u1} is the key generated for the local SA shared between the MU and the LAS, $ALGORITHM$ is the description of the algorithm for the local SA selected by the HAS that will be used for local authentication, F_i is a random number used to avoid replay attack between AAA servers i and $i-1$ in the AAA chaining servers shown in Fig. 4, F_0 is a random number used to avoid replay attack between the MU and the LAS, K_0 is the pre-shared key in the SA between the MU and its HAS, K_i is the pre-shared key in the SA between AAA servers i and $i-1$ in the AAA chaining servers shown in Fig. 4, the subscripts K_0 and K_i mean that the data in the parenthesis are encrypted with K_0 or K_i, respectively.

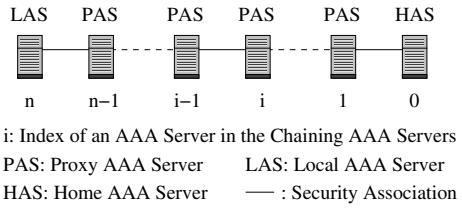

Fig. 4. Demonstration of Chaining AAA Servers.

When the LAS receives an authentication approval with the message shown in (2), the LAS decrypts the message with the key and algorithm in the SA shared with the upstream PAS and replies value $F_n - 1$ to the PAS to avoid replay attack, where n is the total number of chaining AAA servers between the LAS and HAS. Then, the LAS sends a message $\{R_1, ALGORITHM, F_0\}_{K_0} \| \{LIFETIME\}_{K_{u1}}$ to the visiting MU, where $LIFETIME$ is the life time of the local SA and it is equal to the residence time of the MU. When the visiting MU receives the message $\{R_1, ALGORITHM, F_0\}_{K0} \| \{LIFETIME\}_{K_{u1}}$, the MU decrypts the first part of the message to obtain the value R_1 and generates the key K_{u1} with (1). With key K_{u1}, the value of $LIFETIME$ is obtained. Then, the MU replies a value of $F_0 - 1$ to avoid replay attack.

After the above operations are finished, a local SA can be established at the visiting MU and the LAS as follows:

SA::={UID; SPI; ALGORITHM; DIRECTION; KEY; LIFETIME},

where UID is the *unique user identification*, which indicates the user for whom the local SA is used. In the local SA at the LAS, UID is the identification of the MU. In the local SA at the MU, UID is the identification of the LAS. SPI (Security Parameter Index) is the identification number of the association, which is used to differentiate the SAs uniquely. ALGORITHM is a description on a specific algorithm that should be used with this local SA. DIRECTION specifies the association used for packets arriving or leaving, KEY provides the encoding and decoding key for the authentication, which is $K1$ in our proposed protocol. LIFETIME is a time period to keep the SA, which is determined and transfered by the LAS.

From the protocol, we can see that the security to distribute the key K_{u1} is guaranteed. First, the messages transmitted between the AAA servers are encrypted with a pair of SAs with nonce technique. Thus, information secrecy and data integrity are provided and replay attack can be defeated. Second, the transmission of key K_{u1} to the visiting MU from the HAS is protected through a random value R_1 with an SA shared between the MU and its HAS, which avoids direct key distribution on the unprotected medium and guarantees secure transmission of K_{u1} from the HAS to the MU.

The threshold value of the residence time that triggers proposed scheme is critical to the authentication efficiency. When the residence time of the MU is greater than the threshold value, the authentication requests come within the life time of the local SA can be processed efficiently since the residence time of the MU is equal to the life time of the local SA. When the residence time of the MU is less than the threshold value, no local SA is established for the visiting MU. All the authentication requests sent by the visiting MU will be authenticated remotely through the AAA architecture, which will impose more burden to the network. Therefore, we propose an authentication cost function next to derive the threshold value of the residence time.

C. Determine the Threshold Value of Residence Time

In order to determine the threshold value of the residence time to trigger the proposed scheme, we evaluate the authentication cost with a accumulated authentication cost function first, which is related with the traffic and mobility patterns as well as the distance between the LAS and the HAS.

Accumulative authentication cost, C_T, is defined as the sum of signaling and encryption/decryption cost for all authentications sent by an MU when it is in a network. C_T depends on the residence time and arrival rate of authentication requests of the MU because they determine the number of authentications in a network. In addition, the distance between the LAS and the HAS in terms of hops has a direct effect on C_T. Therefore, C_T can be written as:

$$C_T = c_{ms}\lambda\tau + (n-1)c_{ss} + c_o, \tag{3}$$

where λ is the arrival rate of the authentications of the MU, c_{ms} is the authentication cost on the hop between the MU and LAS, c_{ss} is the authentication cost on the hop between authentication servers, n is the number of hops between the MU and its HAS. c_o is the maintenance cost for a local SA at the LAS. τ is a mean value of the residence time of the MU in a network. The first part of C_T is the authentication cost for the MU after the establishment of local SA. The second part of C_T is the cost to establish a local SA for the MU.

Assume that the existing authentication scheme is DIAMETER. In order to trigger our proposed scheme to replace it, C_T should be at least less than the authentication cost with remote authentication in DIAMETER. Let C_p be the authentication cost with remote authentication, C_p can be obtained as:

$$C_p = [(n-1)c_{ss} + c_{ms}]\lambda\tau. \tag{4}$$

By comparing (3) and (4), the threshold value of the residence time, i.e., τ_{th}, of an MU can be carried out as:

$$\tau_{th} = \frac{1}{\lambda}\left[\frac{c_o}{(n-1)c_{ss}} + 1\right]. \tag{5}$$

If the residence time of an MU, i.e., τ, is greater than the threshold, τ_{th}, our scheme is triggered to establish the local SA for efficient authentication and assign the value of τ to the life time of the SA. Otherwise, DIAMETER is used at the LAS in the AAA architecture.

We also evaluate the authentication latency per operation with proposed scheme. The *authentication latency per operation* is defined as a time period from when an MU sends out a request to when the MU receives the request response. Denote the authentication latency per operation as T, which can be evaluated as:

$$T = \begin{cases} t_{ms}, & \text{if SA exists} \\ t_{ms} + nt_{ss}, & \text{if SA does not exist} \end{cases}, \tag{6}$$

where t_{ms} is the authentication time on the hop between the MU and LAS, t_{ss} is the authentication time on the hop between authentication servers. Next, we compare C_T and T with DIAMETER to show the advantage of proposed scheme.

IV. Numerical Results

In this section, we introduce the simulation scenario and the parameters for numerical results first. Then, the authentication cost and latency are evaluated and compared to those with DIAMETER based on different conditions.

In our simulation, the parameters needed to evaluate the authentication cost and latency are shown in Table I. We use the number of signaling messages for authentication to evaluate the authentication cost c_{ms} and c_{ss}. Therefore, from Fig. 3, we can obtain $c_{ms} = 4$ and $c_{ss} = 2$. As for authentication latency, since the transmission delay is dominant in secret-key-based authentication, we use the delay to transmit an authentication message to represent the authentication latency. When the maximum authentication message size is 4096 bytes [7], the transmission delay for one signaling message is about 16 milliseconds with the assumption of 2 Mbps link capacity [3]. Therefore, $t_{ms} = 64ms$ and $t_{ss} = 32ms$. The default values of n, λ, and τ are set as 4, 0.3, and 10, respectively. In the

TABLE I

SIMULATION PARAMETERS.

c_{ms}	c_{ss}	t_{ms} (ms)	t_{ss} (ms)	n	λ (min^{-1})	τ (min)
4	2	64	32	4	0.3	10

following figures, when we change any one of these three parameters, the other two will be kept at the default values.

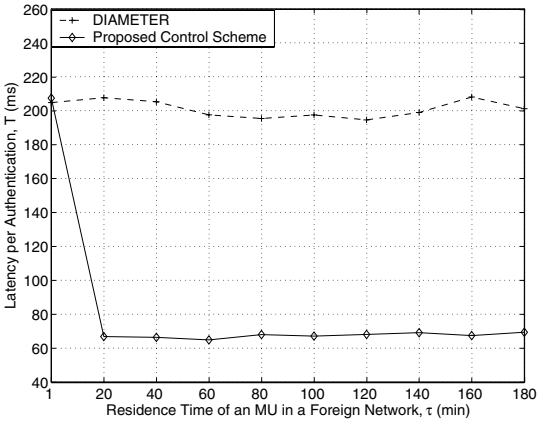

Fig. 5. Authentication Time vs. Residence Time of an MU.

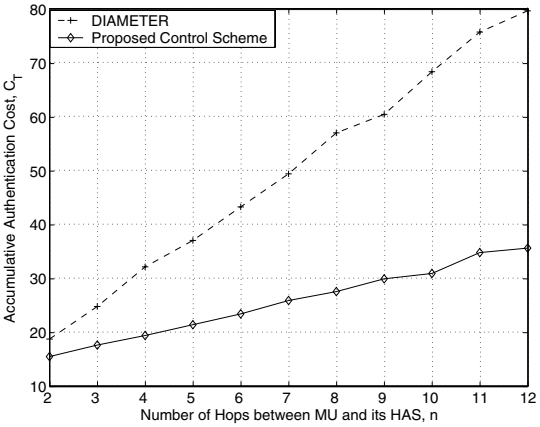

Fig. 6. Authentication Cost vs. Number of Hops.

Based on these parameters, we evaluate and compare authentication latency per operation and accumulative authentication cost with DIAMETER. The results are shown in Fig. 5, 6, and 7. In Fig. 5, the improvement of authentication latency per operation with proposed scheme is about 68%. The improvement comes from the use of local SA to authenticate the visiting MU. Since the remote authentication is changed to local authentication, the authentication latency is reduced greatly. In Fig. 6, we can see that the improvement of accumulative authentication cost is increasing with the increase of the number of hops between the MU and its HAS. At the point of nine hops, the proposed scheme costs 50% less than the DIAMETER. The benefit also comes from the utilization of local SA for authentication. In Fig. 7, although the authentication cost increases with the increase of arrival

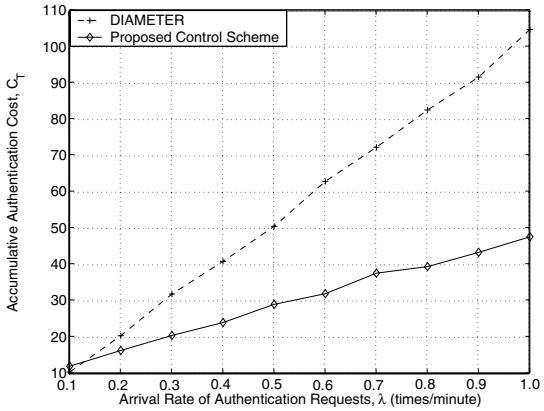

Fig. 7. Authentication Cost vs. Arrival Rate of Authentication Requests.

rate of authentication requests in both cases, the cost with proposed control scheme is less than that with DIAMETER with 40% improvement at the point of $\lambda = 0.5$.

V. CONCLUSION

In this paper, we propose a local authentication control scheme which can be implemented in any wireless networks with AAA architecture. By establishing a local security association with concern of traffic pattern, mobility pattern, and number of hops between the mobile user and its home authentication server, the proposed scheme becomes a promising alternative for secure and efficient authentication approach in various wireless networks.

REFERENCES

[1] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, and S. Miller, "The Evolution of Wireless LANs and PANs - Efficient Authentication and Key Distribution in Wireless IP Networks," *IEEE Personal Communications on Wireless Communications*, vol. 10, pp. 52–61, December 2003.

[2] V. Gupta, S. Gupta, and S. Chang, "Performance Analysis of Elliptic Curve Cryptography for SSL," in *WiSe'02-ACM Workshop on Wireless Security*, September 2002.

[3] A. Hess and G. Schafer, "Performance Evaluation of AAA / Mobile IP Authentication," in *http://www-tkn.ee.tu-berlin.de/publications/papers/pgts2002.pdf*, 2002.

[4] H. Kim and H. Afifi, "Improving Mobile Authentication with New AAA Protocols," in *IEEE International Conference on Communications*, vol. 1, pp. 497–501, 2003.

[5] S. Shieh, F. Ho, and Y. Huang, "An Efficient Authentication Protocol for Mobile Networks," *Authentication Protocol Journal of Information Science and Engineering*, vol. 15, pp. 505–520, 1999.

[6] S. Glass, T. Hiller, S. Jacobs, and C. Perkins, "Mobile IP Authentication, Authorization and Accounting Requirements," *RFC2977*, October 2000.

[7] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter Base Protocol," *draft-ietf-aaa-diameter-17.txt*, December 2002.

[8] W. Stallings, "Network Security Essentials," *Applications and Standards*, 2000.

[9] T. Dierks and C. Allen, "The TLS Protocol," *rfc2246*, January 1999.

[10] C. Perkins and P. Calhoun, "Mobile IPv4 Challenge/Response Extensions," *RFC3012*, November 2000.

[11] T. Braun, L. Ru, and G. Stattenberger, "An AAA Architecture Extension for Providing Differentiated Services to Mobile IP Users," *Proceedings. Sixth IEEE Symposium on Computers and Communications, 2001.*, pp. 472–478, 2001.

[12] I. Chen and N. Verma. Simulation Study of a Class of Autonomous Host-Centric Mobility Prediction Algorithms for Wireless Cellular and Ad Hoc Networks. In *36th Annual Simulation Symposium*, pages 65–72, 2003.