A Cost-Aware Control Scheme for Efficient Authentication in Wireless Networks

Wei Liang   Wenye Wang
Department of Electrical and Computer Engineering
North Carolina State University, Raleigh, NC 27695

Abstract— **In this paper, we propose a cost-aware control scheme to realize efficient authentication in wireless networks based on the user density, mobility, and traffic patterns of roaming users. First, a mechanism to establish and break a direct security association (SA) between two networks is introduced. Then, an authentication cost function is developed to measure the cost for the proposed scheme. We further investigate an optimal condition to minimize the authentication cost, which decides the optimal number of inter-domain authentication requests to establish direct SAs between networks. Finally, we analyze the optimal condition based on user density, mobility, and traffic patterns. Compared to the authentication without control scheme, the proposed scheme reduces the authentication cost greatly with the increasing number of hops, residence time of mobile users, and the arrival rate of inter-domain authentication requests.**

I. Introduction

The rapid growth of wireless networks enables convenient access to the Internet while demanding delicate design of security services due to the open mediums in mobile environments [1]. In order to provide secure service over wireless networks, many security mechanisms are proposed [2], [3], [4], in which authentication is a process to identify mobile nodes (MNs) when MNs are roaming. The inter-domain authentication in wireless networks must depend on an existing authentication architecture to transfer verification data to the home authentication server (HAS) of the MN so that either end-to-end security association (SA) or hop-by-hop SA can be maintained between local authentication server (LAS) and HAS. In IP security architecture (IPsec), SA is defined as a one-way relationship between a sender and a receiver that affords security services to the traffic. Application of end-to-end SAs between *each pair* of authentication servers (ASs) is proven to be a problem in wireless networks due to the quadratic growth of the number of SAs with an increase in the number of wireless network [5]. Therefore, IETF proposes chaining architecture to authenticate roaming MNs with the advantage of scalability [6]. The application of chaining architecture can maintain hop-by-hop SAs. However, the configuration of hop-by-hop SAs may encrypt and decrypt the data multiple times during the authentication. If there are many proxy authentication servers (PASs) between two end servers, the authentication cost will increase significantly due to the multiple encryption and decryption of data.

To provide efficient authentication in this scenario, IETF suggests PASs assist in setting up direct SAs between two wireless networks based on their mutual interests [6]. However, it is also admitted in [6] that this solution will induce additional initialization costs to the authentication system. Meanwhile, the mutual interests and time point to establish a direct SA between two wireless networks are not clearly defined. Therefore, we need to control the direct SAs established between two wireless networks intelligently, according to clearly defined mutual interests, and minimize the cost of this process. To this end, we propose a cost-aware control scheme for efficient authentication in wireless networks, which is able to establish direct SAs between wireless networks according to user density, mobility, and traffic patterns. Moreover, the cost of establishing direct SAs is minimized in the proposed scheme by choosing an optimal number of networks to set up direct SAs.

The rest of this paper is organized as follows. Section II introduces the background of authentication in wireless networks. In Section III, we propose the cost-aware control scheme for efficient authentication, which minimizes the authentication cost based on user density, mobility and traffic patterns. In Section IV, we evaluate the performance of the proposed control scheme on authentication cost. Then, simulation results are provided with comparison of the authentication without control scheme in Section V. Finally, we draw a conclusion in Section VI.

II. Background of Authentication in Wireless Networks

In this section, we first introduce the authentication in wireless networks. Then, hierarchical authentication architecture and the establishment of direct SAs between networks are described as the basis of the proposed control scheme.

A. Authentication in Wireless Networks

In wireless networks, authentication is defined as a process to identify an MN when it requests service. A common authentication scheme widely used in wireless networks is the challenge/response mechanism [3], in which an MN sends out an authentication request to LAS when it is requesting service in a foreign network. Then, a challenge value is produced by LAS and sent back to the MN. The MN replies a response value by encrypting the challenge value with the SA shared with its HAS. LAS delivers the request, the challenge value, and the response value to the HAS of this MN. The HAS verifies the response value to the challenge value with the same SA as the MN owns. If the values match, the MN is authenti-

0-7803-8523-3/04/$20.00 ©2004 IEEE.

cated and an authentication approval is sent back to the LAS. Otherwise, the authentication request is rejected.

To guarantee the security of transmission, LASs depend on an architecture to deliver the messages for authentication. Since chaining ASs are widely used for secure delivery of the messages, a hierarchical authentication architecture is built up with the ASs, which is introduced next.

B. Hierarchical Authentication Architecture

A hierarchical authentication architecture (HAA) is proposed in [6], where there is one central LAS in a wireless network to take charge of authentication. An LAS shares an SA with a PAS, which is used to manage the SAs of a group of LASs. The PASs are organized in groups and are controlled by a higher-level PAS, which greatly reduces the number of SAs. Due to this advantage, the HAA is deployed widely in wireless networks and proposed by IETF as a recommended standard for Mobile IP networks [6].

However, the HAA does not provide end-to-end protection between two LASs due to the lack of direct SA between them. Instead, it provides hop-by-hop protection for authentication, which causes the authentication data to be encrypted and decrypted multiple times. In terms of hops, if the distance between two LASs is long, the multiple encryption and decryption will cost much in the authentication system. Although [6] suggests PASs assist in establishing direct SA between two LASs with mutual interests, it also admits that this operation induces additional cost to networks. In addition, the mutual interests and time point to set up the direct SA between two networks are not clearly described.

In order to provide a clear direct SA establishment scheme with concern of clearly defined mutual interests and authentication cost, we propose a cost-aware control scheme in Section III. But first, we will introduce the concept of SA and the method to establish a direct SA in our proposed scheme.

C. Security Association and Establishment Protocol

As defined in IPsec, the security association (SA) is a one-way relationship between a sender and a receiver that affords security services to the traffic. It has many parameters, such as security parameters index (SPI), keys and lifetime, all of which can be used to indicate an encryption and authentication method [7]. Whenever the SA is established and modified, these parameters can be modified simultaneously by using Internet security association and key management protocol (ISAKMP), secure socket layer (SSL) or transport layer security (TLS). Of these protocols, SSL and TLS are two protocols commonly used in wireless networks. SSL is a standard for encrypted client/server communication between network devices, working with a public key to encrypt and transfer data. TLS is an IETF standard with the goal to produce an Internet standard version of SSL [8]. A four-way handshake protocol in TLS allows two LASs to negotiate encryption algorithms and exchange keys to set up an SA before any application data is transmitted.

In our proposed scheme, we depend on the HAA to relay critical information on direct SAs between two LASs, and we apply a four-way handshake protocol in TLS to exchange the key and related information for the direct SA. After the process, the direct SA is established.

III. Cost-Aware Control Scheme for Efficient Authentication

In this section, we propose a cost-aware control scheme for efficient authentication in wireless networks. First, we illustrate the process of the proposed scheme. Then, we evaluate the authentication cost with this scheme and provide an optimal condition to minimize authentication cost based on user density, mobility and traffic patterns.

A. Design of Cost-aware Control Scheme

In the proposed scheme based on HAA, we investigate the authentication in a wireless network. The scheme demands the LAS in the network periodically detecting the number of users, mobility and traffic patterns from different networks. The mobility and traffic patterns in the proposed scheme are presented with residence time and individual arrival rate of authentication requests, respectively. If the total number of authentication requests of MNs from foreign network i within time T, denoted as $L_i(T)$, is greater than a threshold value L^*_{iT}, our proposed scheme will enable the LAS in current network w to set up a direct SA with network i using a four-way handshake protocol in TLS. $L_i(T)$ can be written as:

$$L_i(T) = \sum_{k_i=1}^{K_i(T)} a_{k_i}(T) t_{k_i}(T) \tag{1}$$

where k_i is the index of inter-domain roaming MNs from network i to the network we are investigating, T is observation time, $K_i(T)$ is the number of inter-domain roaming MNs that come from network i and pass or stay at network w within time T, $a_{k_i}(T)$ is an individual arrival rate of authentication requests generated by MN k_i, and $t_{k_i}(T)$ is the residence time of MN k_i observed in time T.

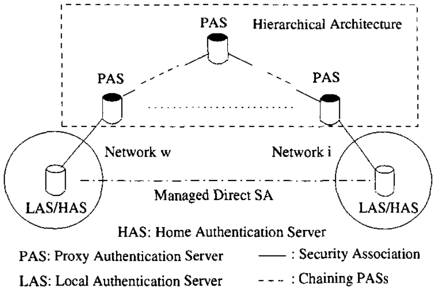
PAS
Hierarchical Architecture
PAS
PAS
Network w
Network i
LAS/HAS
Managed Direct SA
LAS/HAS
HAS: Home Authentication Server
PAS: Proxy Authentication Server
—— : Security Association
LAS: Local Authentication Server
- - - : Chaining PASs

Fig. 1. Cost-Aware Control Scheme on Hierarchical Architecture

An example of the proposed scheme working on HAA is shown in Fig. 1, in which the LAS in network w performs the proposed scheme as follows:

1. In network w, LAS periodically detects $K_i(T)$, $a_{k_i}(T)$ and $t_{k_i}(T)$ of the users from network i, which represent the mutual interests between network w and i.
2. LAS in network w calculates the value of $L_i(T)$ for network i and compares it to the threshold value L^*_{iT}.

3. If $L_i(T)$ is greater than the threshold value L_{iT}^*, LAS in network w initiates a four-way handshake protocol to set up a direct SA with network i serving for next time period T.
4. If $L_i(T)$ is less than the threshold value L_{iT}^*, LAS in network w sends all of the authentication requests of users from network i to the PAS trusted by the LAS in network w.

From these steps, we can see that L_{iT}^* is critical to the proposed scheme with great effect on the performance. Therefore, we analyze the authentication cost with and without our control scheme in the following paragraphs, and derive the optimal value of L_{iT}^* based on the analysis.

B. Optimal Value of L_{iT}^*

In order to obtain the optimal value of L_{iT}^*, first we need to derive the cost function with and without proposed authentication control scheme.

Assume the authentication costs for one inter-domain roaming authentication request *with* and *without* direct SA between networks w and i are $c^{(s)}$ and $c^{(l)}$, respectively. And, if we define $C^{(s)}$ and $C^{(l)}$ as the total authentication cost function with and without the proposed scheme in time T, respectively, $C^{(l)}$ and $C^{(s)}$ can be written as:

$$C^{(l)} = L_i(T)c^{(l)}, \quad C^{(s)} = L_i(T)c^{(s)} + c^{(I)} + c^{(m)}(T) \tag{2}$$

where $c^{(I)}$ is initialization cost to set up a direct SA between two networks, and $c^{(m)}(T)$ is SA maintenance cost in time T.

In our proposed scheme, when $C^{(l)}$ is less than or equal to $C^{(s)}$, we will initiate our scheme to set up a direct SA for efficient authentication. Therefore, the optimal value of L_{iT}^* can be derived from (2) as follows:

$$L_{iT}^* = \frac{c^{(I)} + c^{(m)}(T)}{c^{(l)} - c^{(s)}}. \tag{3}$$

IV. Evaluation of Authentication Cost

To evaluate the authentication cost with or without our proposed scheme, we need to evaluate the variables, $c^{(l)}$, $c^{(s)}$, $c^{(I)}$ and $c^{(m)}(T)$, as well as $K_i(T)$, $a_{k_i}(T)$ and $t_{k_i}(T)$ in (1).

A. Authentication Cost without Proposed Scheme

An authentication process with challenge/response mechanism involves the encryption of challenge value, transmission of encrypted data, decryption of data and verification of data [3]. When hop-by-hop SA is used for authentication, the data must be encrypted and decrypted one time on each SA. Therefore, assuming encryption, decryption and transmission cost are the same on different hops, $c^{(l)}$ can be written as:

$$c^{(l)} = 2n(c_e + c_d + c_t) + c_v, \tag{4}$$

where c_e is the encryption cost on one hop, c_d is the decryption cost on one hop, c_t is the transmission cost on one hop, c_v is the verification cost on HAS, and n is the number of hops between the LAS in network w and HAS in network i.

B. Authentication Cost with Proposed Scheme

In our proposed scheme, because encryption and decryption are performed twice on one SA, $c^{(s)}$ becomes:

$$c^{(s)} = 2(c_e + c_d) + 2nc_t + c_v. \tag{5}$$

Here, c_e, c_d, c_t, and c_v are the same as those in (4).

However, in our proposed scheme, when the LAS in network w initiates a four-way handshake protocol to set up a direct SA with network i, additional costs are induced, which include the initialization cost and the maintenance cost, which is a function of time. The initialization cost is considered the cost to establish direct SA between two networks with a four-way handshake protocol in TLS. And it is also related to the number of hops between two networks due to the transmission of confidential data for the direct SA. Thus, $c^{(I)}$ is shown as:

$$c^{(I)} = 2n(c_e + c_d + c_t) + 2c_c \tag{6}$$

where n, c_e, c_d, and c_t are described in (4), while c_c is the cost to compute and generate parameters for the direct SA.

$c^{(m)}(T)$ in the proposed scheme is the potential cost to keep the direct SA to continue authenticating the inter-domain roaming MNs. First, the storage of additional SA consumes some local space. Then, with the time increasing, the additional SA might compromise the authentication architecture by increasing the complexity of networks in terms of the number of SAs [5]. Furthermore, an extended existence of an additional SA provides attackers more chances to intrude the network. Therefore, $c^{(m)}(T)$ can be written as:

$$c^{(m)}(T) = c_1 + c_o(T) \tag{7}$$

where c_1 is the storage cost and $c_o(T)$ is the other potential cost within time T, which is defined as:

$$c_o(T) = \int_0^T c_2 e^{\alpha x} dx, \tag{8}$$

where c_2 is a risk or cost value assigned to a security level. Since the concept of security level is widely used in network, environment and power risk assessment [9], [10], we assign two values for two security levels to c_2. When an MN is in its home network, in general, the security level is low, which means the user trusts surroundings, and the risk value is low. When an MN is beyond its home network, the security level is high, and the risk value is accordingly high because the MN may face more threats such as denial of service due to incompatibility in a foreign network. α is a coefficient to specify the speed of risk increase with t.

C. Evaluation of $L_i(T)$ with Mobility and Traffic Patterns

To evaluate $L_i(T)$, we assume a_{k_i} and t_{k_i} are independent identical distribution (IID) to all the inter-domain roaming users from network i. Then, a_{k_i} and t_{k_i} become a_i and t_i. Furthermore, we assume a_i is a Poisson distribution with mean λ_i, t_i is a Gamma distribution with mean τ_i. Since $K_i(T)$ is the total number of inter-domain roaming users, it can be expressed as:

$$K_i(T) = S_w U_i(T), \tag{9}$$

where $U_i(T)$ is the density function of inter-domain roaming users from network i, which is supposed to be Gaussian distribution with mean m_i, and S_w is the area of network w we are studying. Given these parameters, the mean value of $L_i(T)$ can be evaluated as follows:

$$E\{L_i(T)\} = S_w E\{U_i(T)\}E\{a_i\}E\{t_i\} = S_w m_i \lambda_i \tau_i. \quad (10)$$

The condition in (3) then becomes the condition as follows:

$$Set\ up\ direct\ SA\ for\ network\ i,\ if\ S_w m_i \lambda_i \tau_i \geq \frac{c_i^{(I)}+c_i^{(m)}(T)}{c_i^{(l)}-c_i^{(s)}},$$
$$Break\ direct\ SA\ with\ network\ i,\ if\ S_w m_i \lambda_i \tau_i < \frac{c_i^{(I)}+c_i^{(m)}(T)}{c_i^{(l)}-c_i^{(s)}}.$$

Next, we provide the detailed algorithm to perform our proposed scheme based on this condition.

D. Algorithm for Proposed Scheme

The algorithm to apply the condition is shown as follows:

```
if $(mod(SystemTime, T) == 0)$
    $for(i = 1; i \leq Num\_Networks; i++)$
        $SumTime(i) = 0;$
        $SumRequests(i) = 0;$
        $Num\_Users(i) = CheckUsers(Network(i));$
        $for(j = 1; j \leq Num\_Users(i); j++)$
            $ResidenceTime(i,j) = CheckTime(User(i,j));$
            $Num\_Requests(i,j) = CheckRequests(User(i,j));$
            $SumTime(i) = SumTime(i) + ResidenceTime(i,j));$
            $SumReq(i) = SumReq(i) + Num\_Requests(i,j));$
        $AveTime(i) = SumTime/Num\_Users(i);$
        $AveRequests(i) = SumRequests/T/Num\_Users(i);$
        $L(i) = Num\_Users(i) * AveTime(i) * AveRequests(i);$
        $Cth(i) = (cl(i) + cm(i))/(cl(i) - cs(i));$
        if $(L(i) \geq Cth(i))$
            $SetupDirectSA(Network(i));$
            $FLAG\_SA(i) = 1;$
        else if$(FLAG\_SA(i) == 1)$
            $BreakDirectSA(Network(i));$
            $FLAG\_SA(i) = 0;$
```

Fig. 2. Algorithm to Calculate the Condition for Proposed Scheme.

In this algorithm, we set up a time, T, to measure the average values of user distribution, mobility and traffic patterns. We assume the cost of $c_i^{(l)}$, $c_i^{(s)}$ and $c_i^{(m)}$ are known to LAS, which are defined as $cl(i)$, $cs(i)$ and $cm(i)$, respectively, in our algorithm. $User(i,j)$ represents the MN j from network i who stays or passes current network in time T. The function $CheckTime(User(i,j))$ is used to get the residence time of the inter-domain roaming MN j from network i in the current network, $CheckRequests(User(i,j))$ is used to obtain the number of authentication requests sent by MN j from network i in the current network, $SetupDirectSA(Network(i))$ is for establishing the direct SA with network i, and $BreakDirectSA(Network(i))$ is used to set the SA expired by changing its lifetime and sending notification to network i.

TABLE I

SIMULATION PARAMETERS FOR DIFFERENT NETWORKS.

netID(i)	hops	$m_i(/(m^2))$	λ_i (/user/minute)	τ_i (minutes)
1	2	0.3	0.2	30
2	5	0.1	0.4	25
3	4	0.6	0.06	20
4	6	0.7	0.5	40
5	8	0.6	0.1	10
6	7	0.4	0.15	15
7	12	0.7	0.4	45
8	10	0.6	0.3	30
9	4	0.7	0.4	15
10	6	0.2	0.3	20
11	3	0.7	0.25	10
12	15	0.6	0.5	35
13	5	0.1	0.15	20
14	9	0.2	0.35	40
15	14	0.2	0.45	35
16	20	0.8	0.4	25
17	8	0.6	0.3	30
18	9	0.2	0.2	15
19	5	0.3	0.25	10
20	3	0.6	0.15	10

TABLE II

SIMULATION PARAMETERS FOR AUTHENTICATION COST.

c_e	c_d	c_t	c_c	c_v	c_1	c_2	α
3	3	1	12	300	2	2	0.1

V. NUMERICAL RESULTS AND SIMULATIONS

In this section, we introduce the simulation scenario first. Then, the simulation results with and without proposed scheme are illustrated and compared.

A. Simulation Architecture and Parameters

In our simulation, we have twenty wireless networks communicating with the wireless network w, in which we evaluate the authentication cost with the proposed scheme. In the simulation architecture, LAS_w is the LAC associated with the HASs in twenty wireless networks. A large number of MNs from different wireless networks are roaming inside the investigated network. We generate the user mobility patterns, user density functions and user traffic patterns for different networks with the parameters shown in Table ??. The area of the network w is assumed to be $100km^2$, and the cost components discussed in our paper are assumed in TABLE II. In this table, time c_e, c_d, c_v, and c_c are assigned to values according to the corresponding process time from [11] and [12]. c_t comes from the transmission time calculated with our assumptions: one hop between two wireless networks is about 20km, two neighbor LASs are connected via 20Mbps link and authentication message is composed of 128 bytes [11]. The observation time T in our simulation is set to fifty minutes and the simulation time is three hundred minutes.

B. Simulation Results

The simulation results are shown in Figures 3-6. In Fig. 3, the authentication cost with the control scheme is about 17% less than the cost without control scheme. In Fig. 4, we can see that although both of the authentication costs with and without the control scheme are increasing with arrival rate of inter-domain authentication requests, the cost with the control scheme is less than that without the control scheme. Fig. 5 shows the impact of the number of hops between networks on the authentication cost with and without our control scheme. We can see that the authentication cost with our control scheme is always less than that without our control scheme although increasing hops cause the authentication costs to increase. In Fig. 6, the authentication cost increases with the increase of residence time of the MNs in both cases. However, the cost with our proposed scheme is far less than the cost without the control scheme. The improvement in these figures comes from the establishment of direct SAs between networks, which reduces the multiple encryption and decryption cost during authentication.

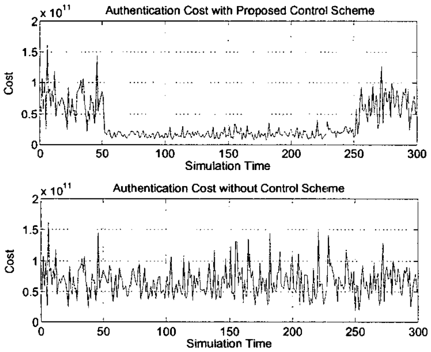

Fig. 3. Authentication Cost in Simulation.

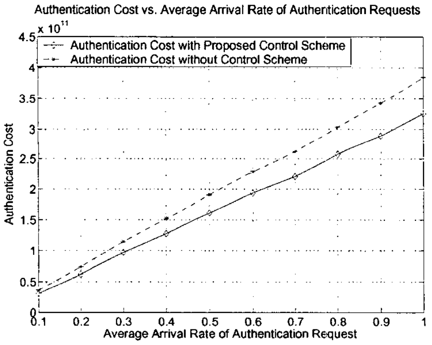

Fig. 4. Authentication Cost vs. Arrival Rate of Authentication Requests.

VI. Conclusion

In this paper, we propose a cost-aware control scheme for efficient authentication among wireless networks. We develop a scheme to manage direct SAs between networks based on an authentication cost function. By minimizing the authentication cost function, an optimal condition can be found to initiate the proposed scheme based on the user density, mobility and traffic patterns. Comparing with the authentication without the control scheme, the proposed scheme demonstrate that the authentication cost is greatly reduced with the increase in the number of hops, arrival rate of inter-domain authentication requests, and residence time of MNs.

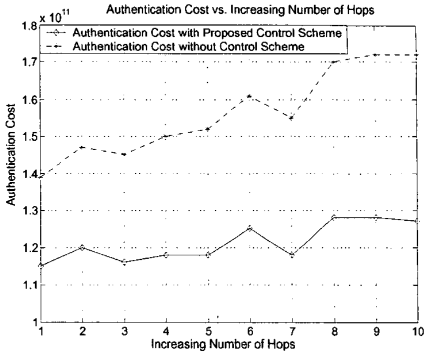

Fig. 5. Authentication Cost vs. Increasing Number of Hops.

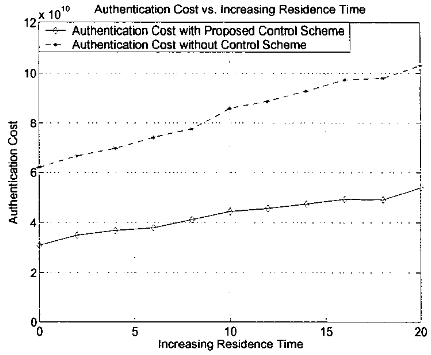

Fig. 6. Authentication Cost vs. Increasing Residence Time.

References

[1] "Wireless Security and VPN, Intel White Paper," *www.intel.com/ebusiness/pdf/prod/relatedmobile/wp023001l.pdf*, 2001.

[2] S. Jacobs, "Mobile IP Public Key Based Authentication," *draft-jacobs-mobileip-pki-auth-02.txt*, March 1999.

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

[4] *IEEE 802.11 Working Group. http://grouper.ieee.org/groups/802/11/ index.html.*

[5] B. Aboba and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming," *RFC2607*, June 1999.

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

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

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

[9] N. Ming, J. McCalley, V. Vittal, and T. Tayyib, "Online Risk-Based Security Assessment," *IEEE Transactions on Power Systems*, vol. 18, pp. 258–265, February 2003.

[10] J. Zou and K. Lu, "Fuzzy Control Applied to Security Level Analysis ," in *TENCOM '02. Proceedings. 2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering*, vol. 2, pp. 28–31, 2002.

[11] 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.

[12] 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.