Registration Scenarios for Wireless LAN MAC Protocol

Frédéric J. Bauchot

CER IBM La Gaude
06610 La Gaude, France

K. S. Natarajan

IBM Thomas J. Watson Research Center
P.O. Box 704, Yorktown Heights, NY 10598

Abstract

In this contribution we propose a high level scenario of the registration procedure taking place between an Access Point and a Mobile Station. Security features such as Authentication, Access Control and data masking key exchange are addressed. For purposes of exposition, this contribution is presented in the context of the medium access control protocol for Wireless LANs proposed in [1].

Introduction

Consider the operation of an autonomous network system (with either multiple Access Points interconnected by a Distribution System, or a single Access Point) complying to the protocol defined in [1]. As previously introduced in this contribution, the *Registration* process corresponds to the procedure by which a Mobile Station introduces itself and requests the services of an Access Point. As far as security is concerned, the services required by the Mobile Station may vary: some options have to be introduced to address the various needs of wireless LANs users. Some of them may be very concerned by the Security and therefore require the safest registration scheme while other users may prefer a simpler (and therefore faster) registration scheme.

In this contribution will be proposed different consistent scenarios to address different levels of security during the registration process.

This contribution is related to Issues 6.1, 6.2, 6.5 and is proposed as an 'Alternative' for Issue 6.4 - Registration [2].

Security options

In this contribution are proposed three different options related to Security:

- The **Authentication Option** is relevant either in Mobile Stations or in Access Points, and can take two values, YES or NO.
  - When equal to YES in an Access Point, an authentication procedure MUST be performed between the Access Point and the Mobile Station

- When equal to NO in an Access Point, an authentication procedure MAY be performed between the Access Point and the Mobile Station (in fact the procedure will be done according to the Mobile Station option).
- When equal to YES in a Mobile Station, an authentication procedure MUST be performed between the Access Point and the Mobile Station
- When equal to NO in a Mobile Station, an authentication procedure IS NOT performed between the Access Point and the Mobile Station

According to the respective values of this option in the Access Point and in the Mobile Station, the authentication will be done or not, and the registration procedure can proceed or not.

The procedures to perform the authentication is not part of this contribution, but it is only assumed that the authentication procedure output is a single variable reflecting either the Success or the reason of failure.

- The **Access Control Option** is relevant in Access Point, and can take two values, YES or NO.
  - When equal to YES in an Access Point, an access control procedure MUST be performed by the Access Point to determine if the candidate mobile station is authorized to enter the network.
  - When equal to NO in an Access Point, an authentication procedure IS NOT performed.

  The procedures to perform the Access Control is not part of this contribution, but it is only assumed that the Access Control procedure output is a single variable reflecting either the Success or the reason of failure.
- The **Data Masking Option** is relevant in Mobile Stations, and can take two values, YES or NO.
  - When equal to YES in a Mobile Station, a procedure MUST be performed between the Access Point and the Mobile station to generate and share a secret key used for data masking.
  - When equal to NO in a Mobile Station, a procedure IS NOT performed.

  The procedures to generate and share a secret key for data masking is not part of this contribution, but it is only assumed that the corresponding procedure output is a single variable reflecting either the Success or the reason of failure.

Note: As the authentication and data masking options apply to mobile stations, it is possible that a given Access Point performs the associated procedures with a first Mobile station, but not with a second one.

Scenarios

The registration procedure is always initiated by a Mobile Station when it decides to enter a network. As described in [1], the Mobile Station must first monitor the radio environment, then choose an Access Point to register with (the criteria of this choice are not addressed by this contribution), and finally issue a **REGISTRATION_REQUEST** control packet (within a slot of the Period C - Contention based Period). This control packet carries the **authentication option** and the **data masking option** among various other parameters.

According to the different options previously introduced, the corresponding procedures are or are not performed.

When any of the former procedures does not complete successfully, then the registration is not successful and must be denied by the Access Point. It is done by issuing a **REGISTRATION_RESPONSE**

control packet (within a slot of the Period A - Broadcast Period) which carries among other parameters a **Result** field reflecting the failure of the whole registration procedure.

When all the performed procedures are successful, then the **Result** field reflects the success of the registration procedure.

If one assume that the procedures previously introduced (authentication, access control and secret key sharing) are performed error free, then the following table shows which ones are done as a function of the **authentication** (both in Mobile station and in Access Point), **access control** and **data masking options**.

Table 1. Security procedures as a function of security options

SCE-NARIO INDEX	SECURITY OPTION				SECURITY PROCEDURE			RESULT
	AP authent. option	MS authent. option	AP access control option	MS data masking option	authenti-cation	access control	share secret key	
1	Yes	Yes	Yes	Yes	Done	Done	Done	Success
2	Yes	Yes	Yes	No	Done	Done	Skipped	Success
3	Yes	Yes	No	Yes	Done	Skipped	Done	Success
4	Yes	Yes	No	No	Done	Skipped	Skipped	Success
5	Yes	No	Yes	Yes	Skipped	Skipped	Skipped	Failure: auth. opt. mismatch
5	Yes	No	Yes	No	Skipped	Skipped	Skipped	Failure: auth. opt. mismatch
5	Yes	No	No	Yes	Skipped	Skipped	Skipped	Failure: auth. opt. mismatch
5	Yes	No	No	No	Skipped	Skipped	Skipped	Failure: auth. opt. mismatch
1	No	Yes	Yes	Yes	Done	Done	Done	Success
2	No	Yes	Yes	No	Done	Done	Skipped	Success
3	No	Yes	No	Yes	Done	Skipped	Done	Success
4	No	Yes	No	No	Done	Skipped	Skipped	Success
6	No	No	Yes	Yes	Skipped	Done	Done	Success
7	No	No	Yes	No	Skipped	Done	Skipped	Success
8	No	No	No	Yes	Skipped	Skipped	Done	Success
9	No	No	No	No	Skipped	Skipped	Skipped	Success

Regardless of the Security aspects, the registration is by itself a procedure that can be either successful or not. Basically it may lead to some process such as resource allocation, or data base update. Those process may be unsuccessful, leading to a deny of the registration request.

The following scenarios give a high level description of the sequence of procedures followed by the pair (Mobile station, Access Point) once the registration process is initiated.

Note: For the purpose of readability, the Acknowledgment packet are not shown in these scenarios. In addition the authentication, access control and data masking options will be respectively referred to as **auth_opt**, **acc_ctrl_opt** and **data_mask_opt** in the rest of this document.

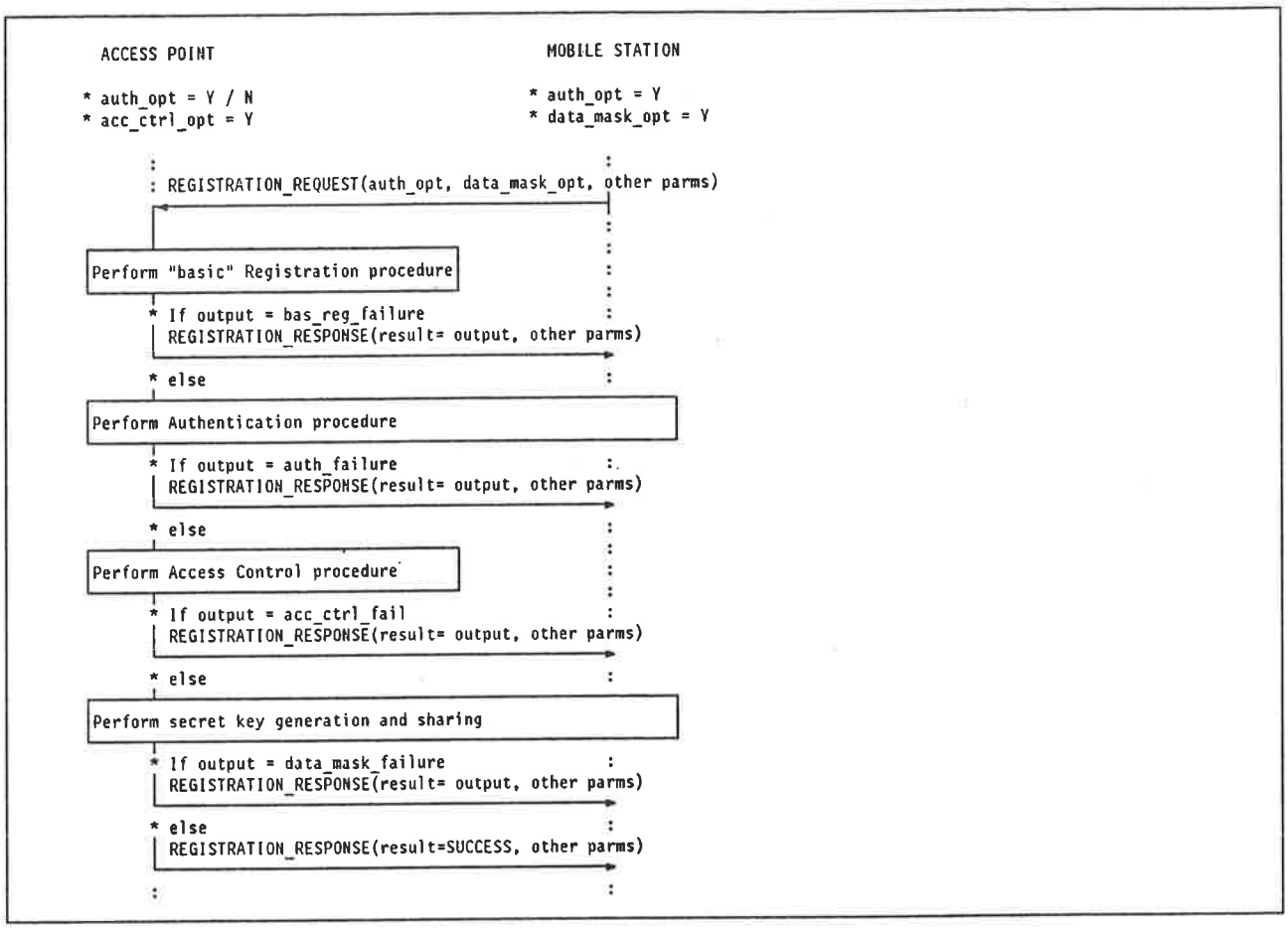

Figure 1. Scenario Nbr. 1

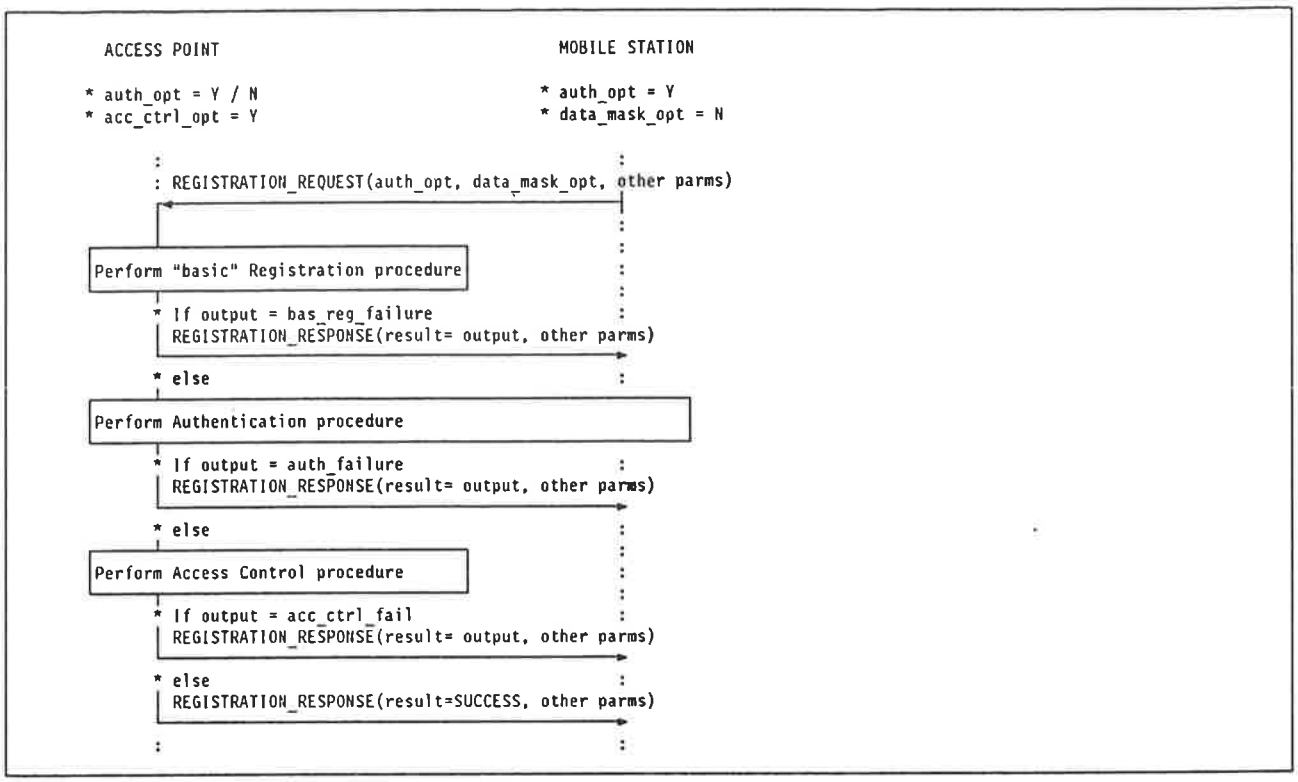

Figure 2. Scenario Nbr. 2

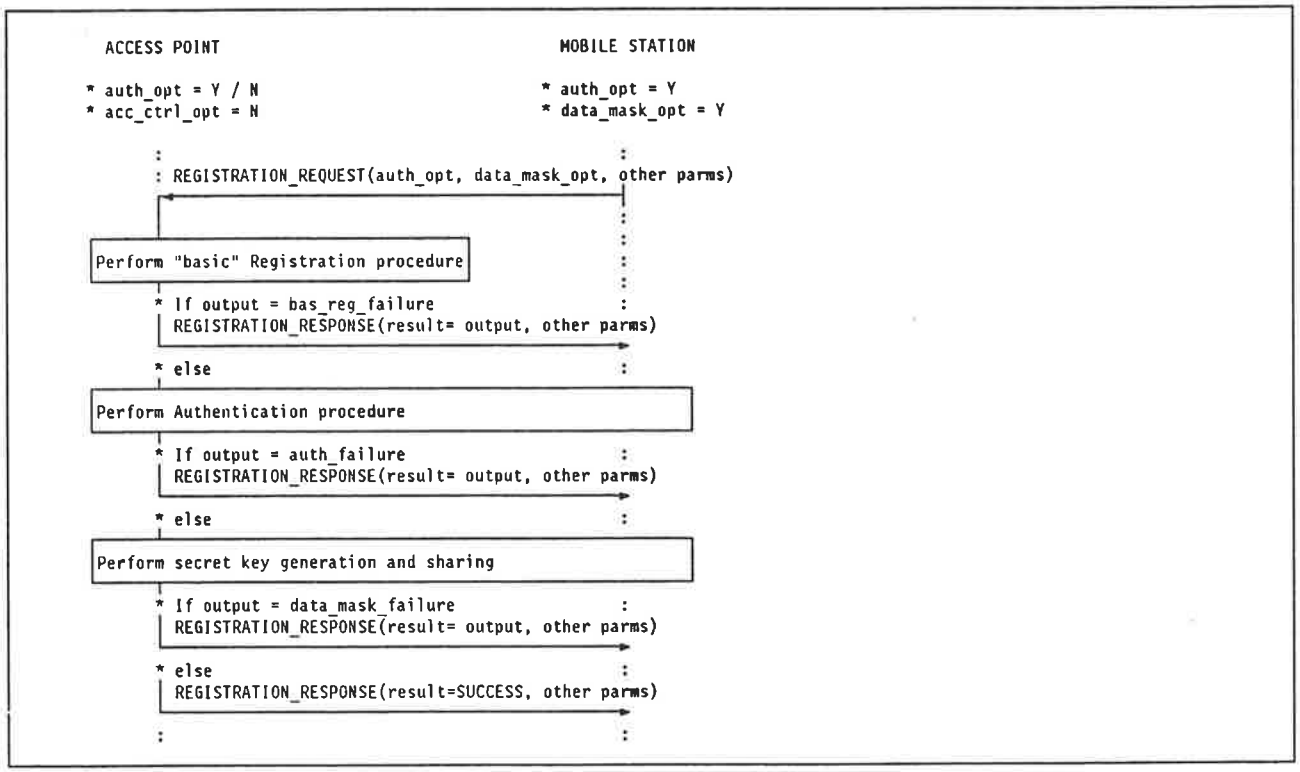

Figure 3. Scenario Nbr. 3

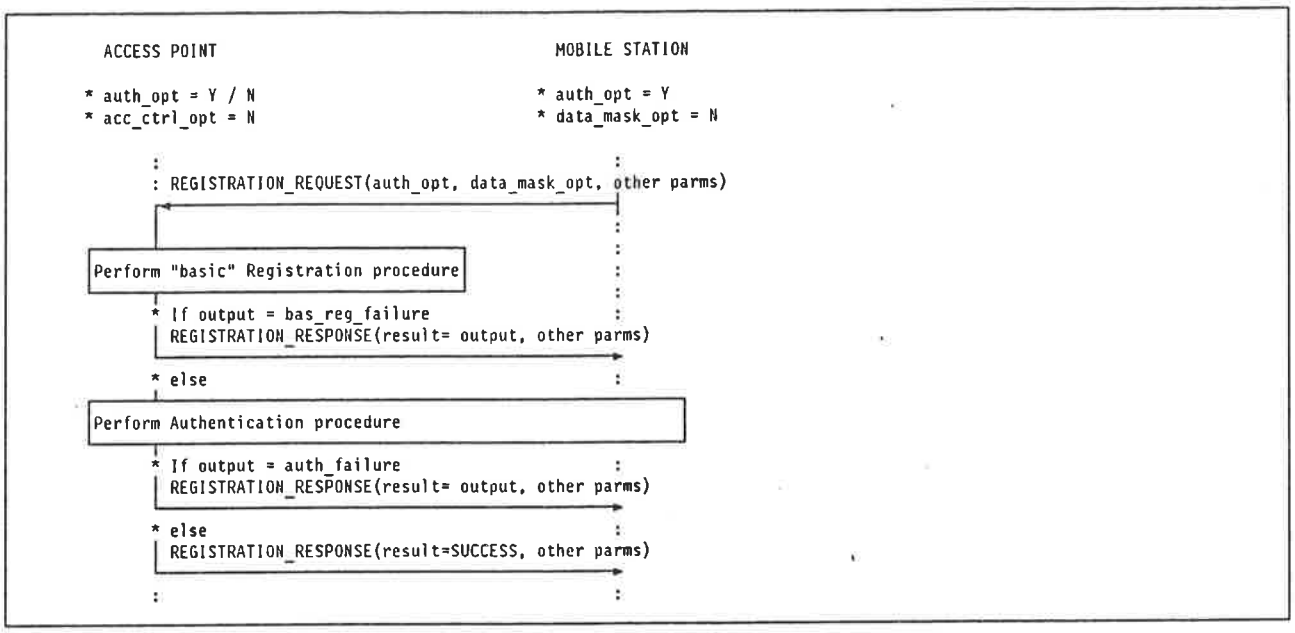

Figure 4. Scenario Nbr. 4

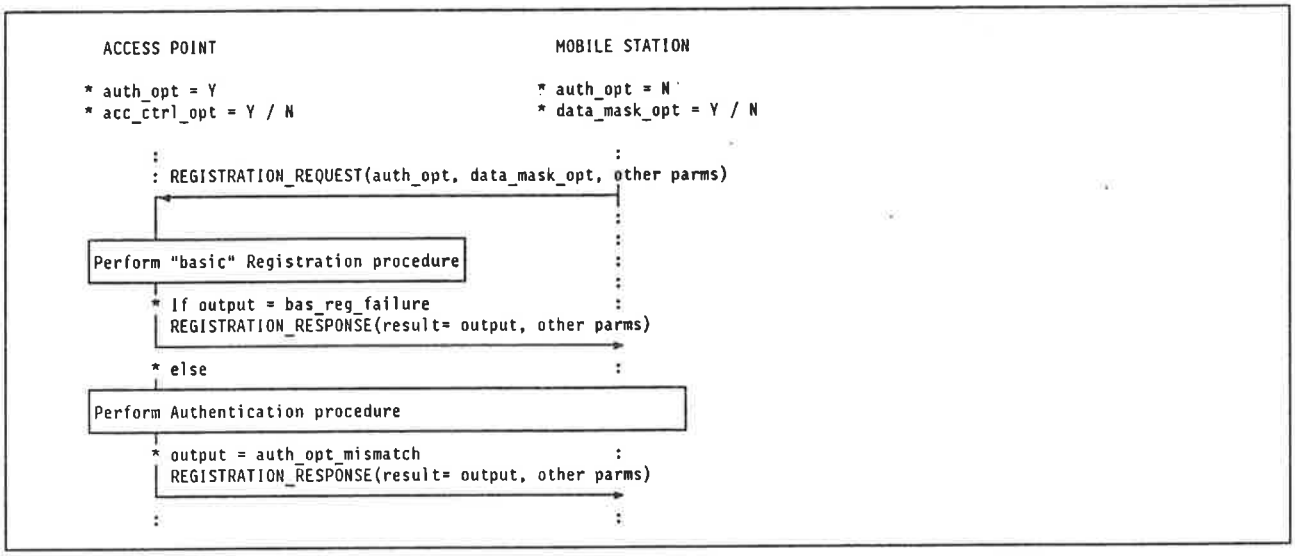

Figure 5. Scenario Nbr. 5

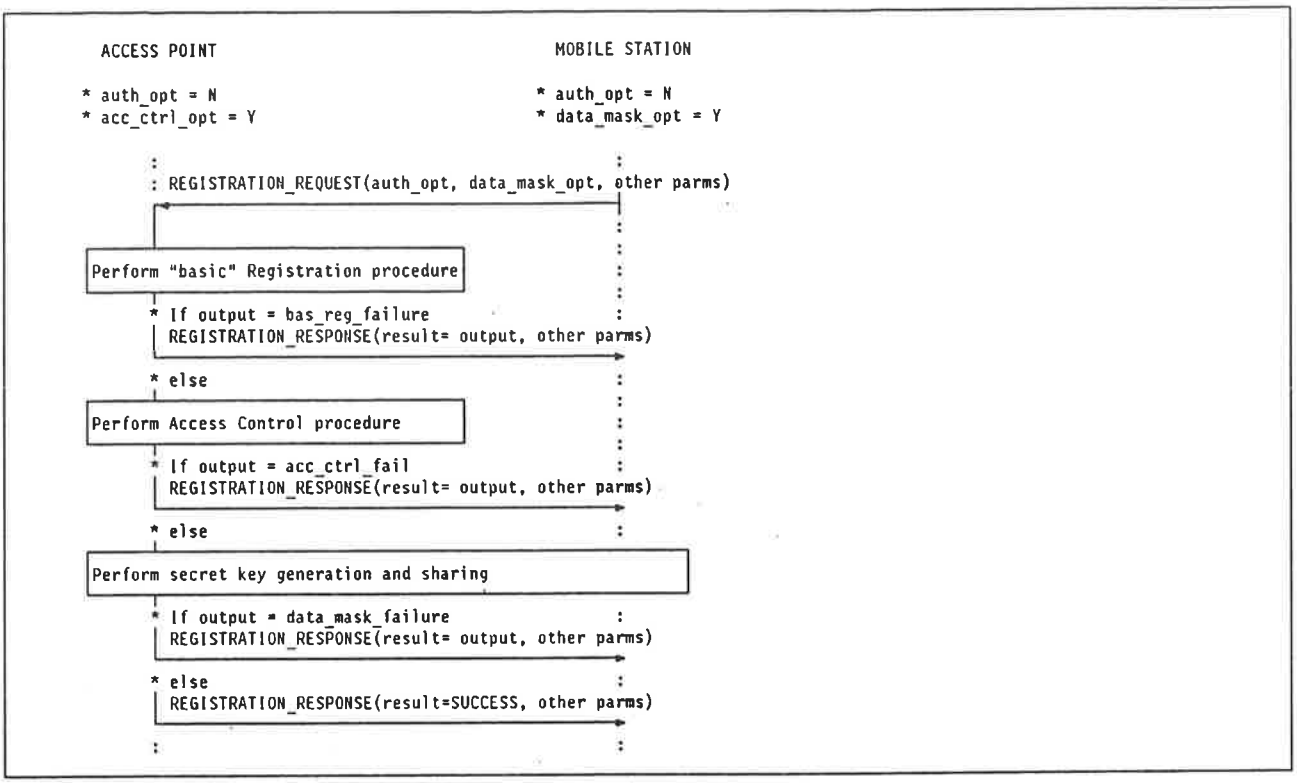

Figure 6. Scenario Nbr. 6

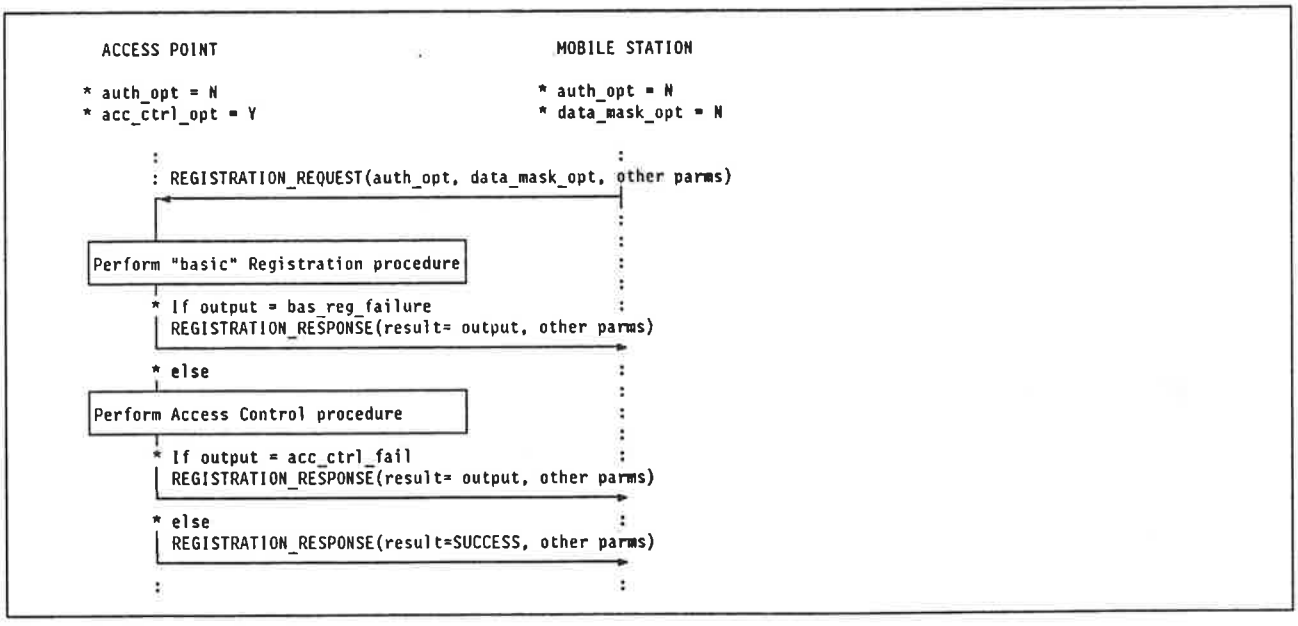

Figure 7. Scenario Nbr. 7

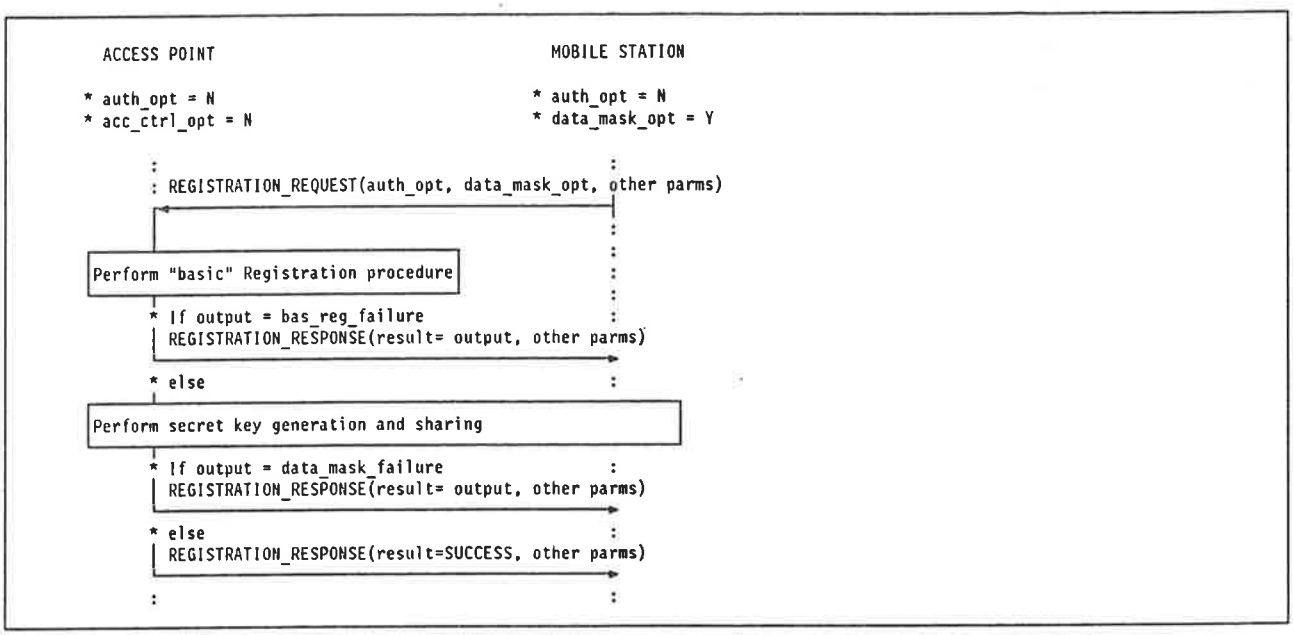

Figure 8. Scenario Nbr. 8

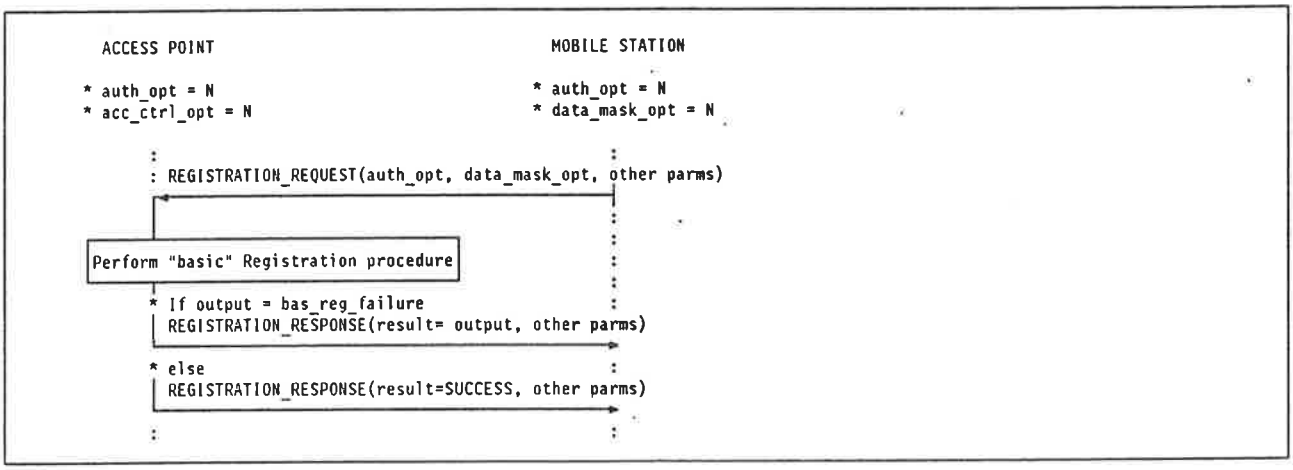

Figure 9. Scenario Nbr. 9

BIBLIOGRAPHY

[1] K.S.Natarajan, C.C.Huang and D.Bantz, *Medium Access Control Protocol for Wireless LANs (an Update)*, IEEE 802.11 Working Group paper, IEEE 802.11/92-39

[2] IEEE P802.11 Issues Document, IEEE 802.11-92/64.