



Secure Wireless Infrastructure Network Using Access Point Checking

Ammar Odeh, Miad Faezipour
 Department of Computer Science & Engineering
 University of Bridgeport, Bridgeport, CT 06604, USA

Abstract

Developments in computers, communication and networks has opened up the doors for wireless network evolution which enjoys attractive features such as dynamic communication and the ease of members to join the network. Improvements in wireless technology has increased the needed for more complicated security systems, where data security and protection represent main wireless networks features.

In distributed systems, the use of networks and standard communication protocols facilitate data transmission between a terminal user and a computer – and between a computer and another computer. Network security measures the need to protect data during transmission. Clearly, wireless networks are less secure compared to wired networks. So, the most important question here is how to protect data transmission in wireless networks.

In this work, we briefly glance at network classes and existing security mechanisms. We then propose our new access point checking algorithm to increase security over infrastructure wireless networks. The goal is to save the time consumed during message travel from one host to another in the network, while maintaining message security. We employ a checksum mechanism to enhance message integrity. In addition, access point (AP) will check the message and decide whether the message should be sent back to the original sender or not. Experimental results for different networking scenarios are provided to validate the system ability. Our technique outperforms traditional security mechanisms in terms of timing characteristics.

Introduction

Nowadays wireless networks are the most popular networks in many environments like universities, banks, and others. Wireless networks provide portability to joint and disjoint users. Another feature is the flexibility that enables connection to new members and/or discarding the connection of others, without the need of any additional hardware equipments.

Networks can be classified into two categories; wired and wireless networks, as shown in Figure 1. This work describes wireless networks and some security issues that play a key role in these networks.

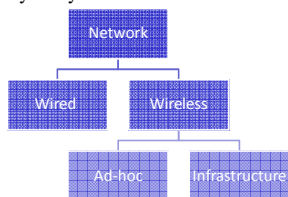


Figure 1. Network classification

Security Mechanisms

A. Open System Authentication: In this protocol, the sender and destination receiver do not share a secret key.

B. Closed Network Access Control: The network administrator will determine the network strategy; whether it is open or closed.

C. Access Control Lists: This is a static mechanism, where a list of MAC addresses for authoritative users are registered before connection setup.

D. Wired Equivalent Privacy Protocol: WEP is a security protocol for local area networks.

Proposed Algorithm

Our proposed algorithm suggests adding checksum to the encrypted message.

In infrastructure wireless networks, the access point (AP) will arrange the connection between two parties and control the connections of all clients in the network. In our method, we add a new duty for AP to check the message and determine if it can be sent, or if it contains unsecure data. This task is performed by applying a checksum bit.

Algorithm Flow Chart

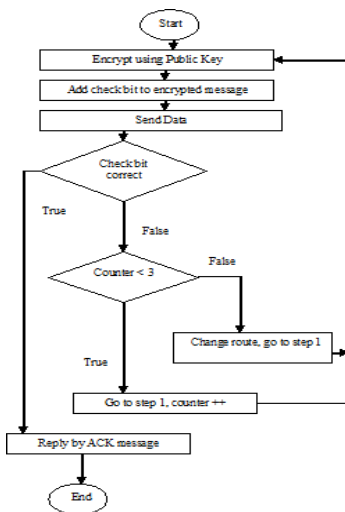


Figure2. Flowchart of the access point check algorithm

Results

The algorithm is rather simple, as it depends on a linear function. Our technique will have the following advantages:

- 1) A more reliable connection will be established compared to the conventional approach, since the unsecure route will be easily discovered. If there is an attacker in the link, it will be discovered and will be removed when the connection is re-established.
- 2) Time will be reduced in case of incorrect message transfers. The time required to deal with incorrect messages is:

$$t_{incorrect} = 2t_{s-ap} + t_{detect}$$

Results (cnt'd)

where:

$t_{incorrect}$: time consumed if message is incorrect.

t_{s-ap} : time consumed from sender to access point.

t_{detect} : elapsed time to detect message status (correct or incorrect).

In the conventional approach; check over plain text, the elapsed time for incorrect messages can be calculated from the following equation:

$$t_{incorrect} = 2(t_{s-ap} + t_{ap-r}) + t_{detect} \quad (7)$$

where:

t_{ap-r} : time required to transfer from AP to the receiver.

Experimental Results for Different Networking Scenarios

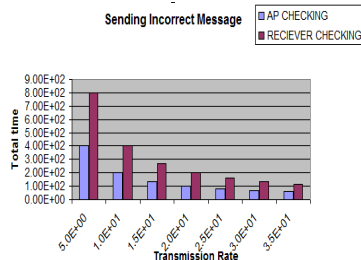


Figure3. Time to detect and reply for incorrect message (transmission rate)

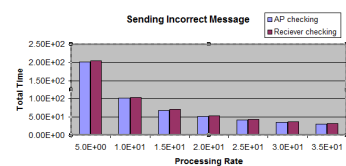


Figure4. Time to detect and reply for incorrect message (Processing rate)

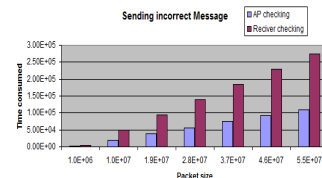


Figure5. Time to detect and reply for incorrect message (Packet size)

Conclusion

Developments in wireless networks require developments in security methodologies to ensure secure data transmission. Furthermore, the time, complexity, and cost should simultaneously be taken into consideration in the design of such security methodologies.