Poster Abstract: An Implementation of Distance-Based Message Authentication for WSNs

Tony Chung and Utz Roedig
InfoLab21, Lancaster University, UK

{a.chunglu.roedig}@lancaster.ac.uk

Abstract. Distance-Based Message Authentication (DBMA) provides an additional layer of access control and helps to defend against key compromise and denial-of-service attacks on constrained nodes. The distance between sender and receiver is measured securely. Messages sent from outside a defined physical distance can be rejected early, protecting vulnerable higher layers. We show our initial implementation using the Nanotron NA5TR1. We show how changing MAC addresses can avoid modification to ranging hardware.

Keywords: round-trip-time, authentication, security, WSNs, denial-of-service.

1 Introduction

WSN security is usually based on cryptography, introducing vulnerabilities such as key-compromise and denial-of-service. Distance-Based Message Authentication (DBMA) is an additional security layer that helps to protect against such attacks without using keys. It measures the distance between a transmitter and receiver during link-layer message exchange and rejects messages from outside a specified distance.

The challenge in any implementation is that the ranging and message transmission must be performed securely and accurately. An attacker should not be able to reduce his apparent range and must not be able to hijack an existing message exchange (i.e. defeating the range measurement entirely).

Our existing theoretical protocol called RTTMAP[1] uses a three-way handshake for each message exchange. It uses the round-trip-time method to calculate the physical separation of nodes. A nonce is utilized during ranging that prevents an attacker from replying early by forcing them to wait for an unpredictable value. A hash commitment is used in the first handshake to prevent an attacker from hijacking an existing exchange.

Our initial analysis considered the Nanotron NA5TR1 transceiver[2] which supports the required ranging accuracy (by using Chirp Spread Spectrum modulation) but is not directly compatible with RTTMAP as data cannot be inserted into ranging packets. Our modified protocol eliminates this requirement by using the standard ranging functions. We still use a hash commitment, but use modified MAC addresses instead of a nonce and transmit the message separately. This paper presents the protocol, a security analysis and our initial findings. We conclude with future work.

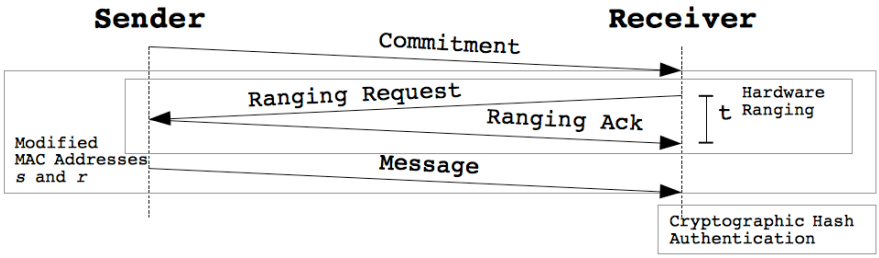

Fig. 1. The Sender sends a commitment to the Receiver. The Sender changes its MAC address using the commitment. The Receiver changes to a random MAC address. The Receiver performs a hardware-based ranging event with the Sender. Finally, the Message is transmitted to the Receiver and is checked against the commitment.

2 Protocol and Security

The objective of the protocol is to reject messages received from outside of a defined physical limit. Other security protocols may still be in place to provide other forms of protection. The following procedure is used for each message exchange (See Fig. 1):

1. The Sender prepares a message *m* in advance (usually including a counter value to prevent replay attack) and hashes it to form commitment *c*.
2. The Sender transmits *c* to the Receiver.
3. *c* is truncated by both parties to form the temporary Sender MAC address *s*.
4. The Receiver generates a random MAC address *r*.
5. The Sender changes its MAC address to *s* and the Receiver changes to *r*.
6. The Receiver initiates a hardware ranging request with the Sender.
7. The Sender returns the ranging acknowledgement.
8. The Receiver aborts if the measured distance exceeds the defined limit.
9. The Sender then sends *m*.
10. The Receiver only accepts *m* if it hashes to *c*.
11. Both nodes reset their MAC addresses.

The hardware ranging is securely combined with message transmission such that an attacker cannot reduce the measured distance, cannot utilize an existing node for the ranging part and cannot hijack an existing message exchange to insert messages.

The MAC change at the Sender prevents the attacker from causing the receiver to initiate a ranging request with a genuine node. The genuine node will not modify its MAC address and therefore will not respond. An attacker could attempt to form a collision, in order to obtain a MAC address that is identical to an existing node. This would be difficult given the necessary structure of a message. Additionally, nodes will not respond to unexpected ranging requests.

The commitment *c* also ensures that the message that is finally transmitted is the same as the one intended for transmission. An attacker would need to find a collision

in *c* in order to hijack an existing genuine message exchange. This is infeasible in the available time.

The MAC change on the Receiver prevents an attacker from arbitrarily sending the ranging acknowledgement early as the destination is not known in advance. The attacker can thus not reduce the distance measurement, without significant hardware modification, due to physical limitation (the speed of light).

3 Implementation and Performance

We have implemented the protocol using the Nanotron DK sensor boards. These comprise of a NA5TR1 Chirp-Spread-Spectrum transceiver and an ATmega128 CPU. Our code utilizes the Nanotron API to control the MAC address, exchange messages, perform ranging and to manipulate transceiver state. We use the Fast Ranging mode, attaining a ranging accuracy of approximately 1m and maximum range of approximately 25m indoors. We show that DBMA is feasible without making hardware changes to the transceiver.

For the hash functionality, we use the SHA-256 function from the MIRACL[3] library. This is truncated when used to set MAC addresses.

4 Conclusion and Future Work

We have shown that the RTTMAP principle can be implemented using standard ranging functionality in existing WSN hardware. Our implementation will be further evaluated to identify detailed ranging accuracy properties as well as performance implications in throughput and energy. Our security analysis will identify if it is vulnerable to existing ranging attacks (such as late-commit), determine the security of the cryptographic primitives used in this context and the analyze potential for attackers to develop hardware to permit a faster turnaround time during ranging. We will also explore the potential for use in other types of network such as WiFi.

References

1. Chung, T., Roedig, U.: On The Feasibility of a New Defense Layer for Wireless Sensor Networks using RF Ranging. In proceedings of the IFIP Network and Service Security Conference, Paris (2009)
2. Nanotron Technologies GmbH: NanoLOC TRX NA5TR1 (2008)
3. MIRACL: Shamus Software (2009)