Ultra-Wideband Location Authentication for Item Tracking

Nathan Rowe[1], Mike Kuhn[1], Brad Stinson[1], Stephen Holland[2]
[1]Oak Ridge National Laboratory, Oak Ridge, TN
[2]Oak Ridge Institute for Science and Education, Oak Ridge, TN

ABSTRACT

International safeguards is increasingly utilizing unattended and remote monitoring methods to improve inspector efficiency and the timeliness of diversion detection. Item identification and tracking has been proposed as one unattended remote monitoring method, and a number of radio-frequency (RF) technologies have been proposed. When utilizing location information for verification purposes, strong assurance of the authenticity of the reported location is required, but most commercial RF systems are vulnerable to a variety of spoofing and relay attacks. ORNL has developed a distance bounding method that uses ultra-wideband technology to provide strong assurance of item location. This distance bounding approach can be coupled with strong symmetric key authentication methods to provide a fully authenticable tracking system that is resistant to both spoofing and relay attacks. This paper will discuss the overall problems associated with RF tracking including the common spoofing and relay attack scenarios, the ORNL distance bounding approach for authenticating location, and the potential applications for this technology.

I. INTRODUCTION

As the nuclear fuel cycle continues to expand both in amount of material and global distribution, it will further tax the limited resources of the IAEA. This threatens to impact the ability of the IAEA to maintain continuity of knowledge (CoK) on material moving within the fuel cycle. At the same time there is a desire to provide more timely detection of material diversions. In order to maintain and improve safeguards effectiveness and eliminate potential vulnerabilities, new tools are needed to improve timeliness of information and increase the efficiency of inspectors.

In order to meet these safeguards needs under a limited budget, the IAEA has placed increasing emphasis on unattended and remotely monitored technologies. These technologies allow the collection of data during periods of inspector absence. In some cases, remote transmission of this data is possible, allowing real-time monitoring of facility activities. These systems increase inspector efficiency by reducing the need for regular on-site inspections and provide inspectors with faster and better-integrated tools to confirm declarations.

To this end, inexpensive, reliable, and secure tagging and tracking methods are needed to provide continuous awareness of material locations, track movement of material between facilities and between processes within facilities, and identify items in combination with information from other unattended monitoring systems. The process of tagging and tracking facilitates information-driven approaches for timely detection by providing near instantaneous status of site inventories and by quickly identifying out-of-place items. A number of radio-frequency (RF) technologies have been proposed for this purpose, but, to date, none have been fielded for routine use.

II. ATTACK SCENARIOS

A 2009 IEEE publication entitled "Open Issues in RFID Security" lists five security threats to radio-frequency identification (RFID): tag cloning, privacy invasion, denial/disruption of service, location-based attacks, and side channel analysis [1]. While these threats are most often considered in the context of passive RFID, which has limited resources to use in addressing them, they can also be applied generally to any wireless tagging and tracking technology. Many of these threats, including tag cloning, privacy invasion, denial/disruption of service, and side channel analysis, have direct parallels in cyber security. In the cyber security realm, most of these attacks are mitigated by common security measures already used in applications like e-commerce and wireless networking. Side channel analysis is unique among these attacks as it is often device or protocol specific. It utilizes information that can be gained indirectly from a device, such as timing delays or power usage. Security measures developed for cyber security can be applied for use in wireless tagging and tracking technology. Location-based attacks, on the other hand, are a unique area of concern for tagging and tracking technologies. Security against these attacks is an area of ongoing research and is a critical need if tagging and tracking technologies are to be adopted for safeguards.

Location-based attacks are an often-overlooked threat to wireless tagging and tracking systems in which an attacker attempts to modify the observed location of a trusted tag. One common implementation of a location-based attack is called a relay attack. Figure 1 demonstrates a relay attack in which the tag is actually located in area 2, but the attacker attempts to make it appear that the tag is in area 1. This is accomplished by blocking the tag RF signal from reaching reader 2 and instead relaying it back into the area of reader 1.

Location-based attacks, like the relay attack, bypass standard cryptographic authentication approaches by relaying communications to and from the original trusted tag. These attacks can be executed against both discrete tracking systems that identify location based on transmit range and against continuous tracking systems that triangulate a tag position in a manner similar to Global Positioning Systems (GPS). Location-based attacks can be as simple as a passive RF relay consisting of only two antennas connected by a cable. More complex methods may be able to convert signals to digital data and relay it long distances via the Internet or satellites.

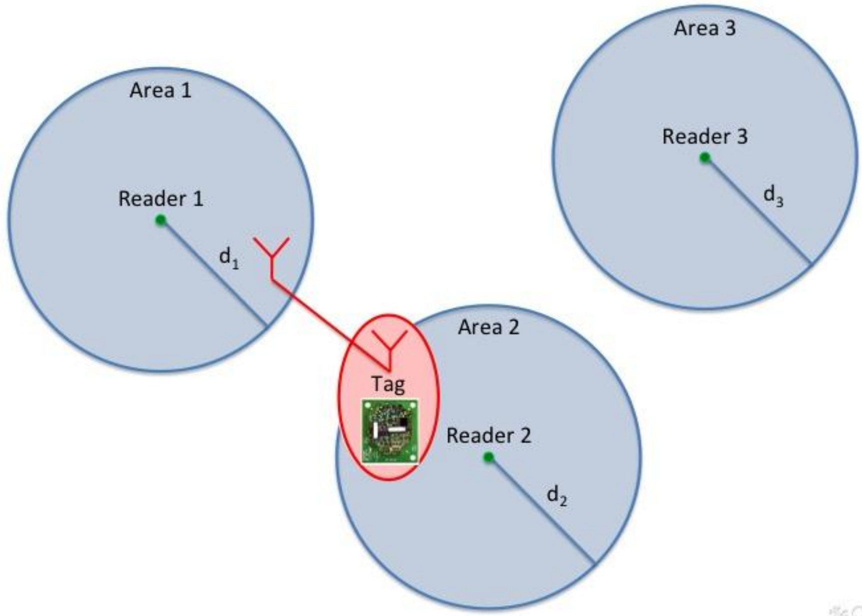


Figure 1: Relay attack in which a trusted tag is made to appear in area 1 while it actually resides in area 2.

III. DISTANCE BOUNDING

Distance bounding methods are the primary technique used for detecting location-based attacks. These methods utilize the return time-of-flight (RTOF) along with the speed of light to calculate an upper bound on the distance of the tag from the reader. The distance is referred to as a bounding distance, because it can only set an upper limit on the tag distance. It is still possible for an adversary to make the tag appear to be farther away than its actual distance from the reader. Figure 2 demonstrates distance bounding in which the total roundtrip time is measured for a signal to propagate from the reader to the tag and then return to the reader as an almost instant reply from the tag. Figure 3 demonstrates the detection of a relay attack using distance bounding. In this figure, the tag is detected as being beyond the range of the reader because of the extended RTOF. Using equation 1, the distance bound of the tag can be calculated as

$$d = c\,\frac{t_1 + t_2}{2}, \qquad (1)$$

where d is the distance bound in meters, c is the speed of light, t_1 is the transmit time from the reader to the tag, and t_2 is the transmit time from the tag to the reader. A number of theoretical studies analyzing distance bounding have been conducted, and several viable protocols have been developed [2],[3].

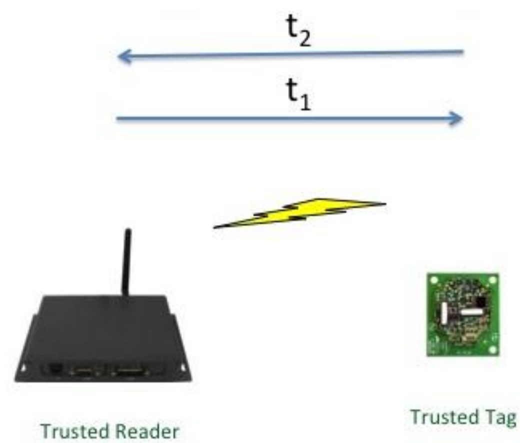


Figure 2: Return time-of-flight measurement for distance bounding under normal conditions.

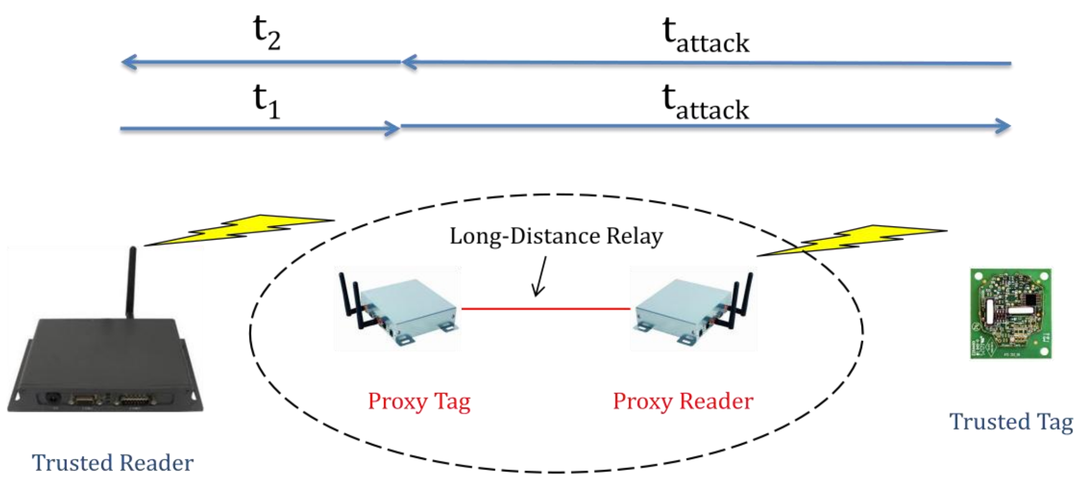


Figure 3: Detection of a relay attack by distance bounding using a return time-of-flight measurement.

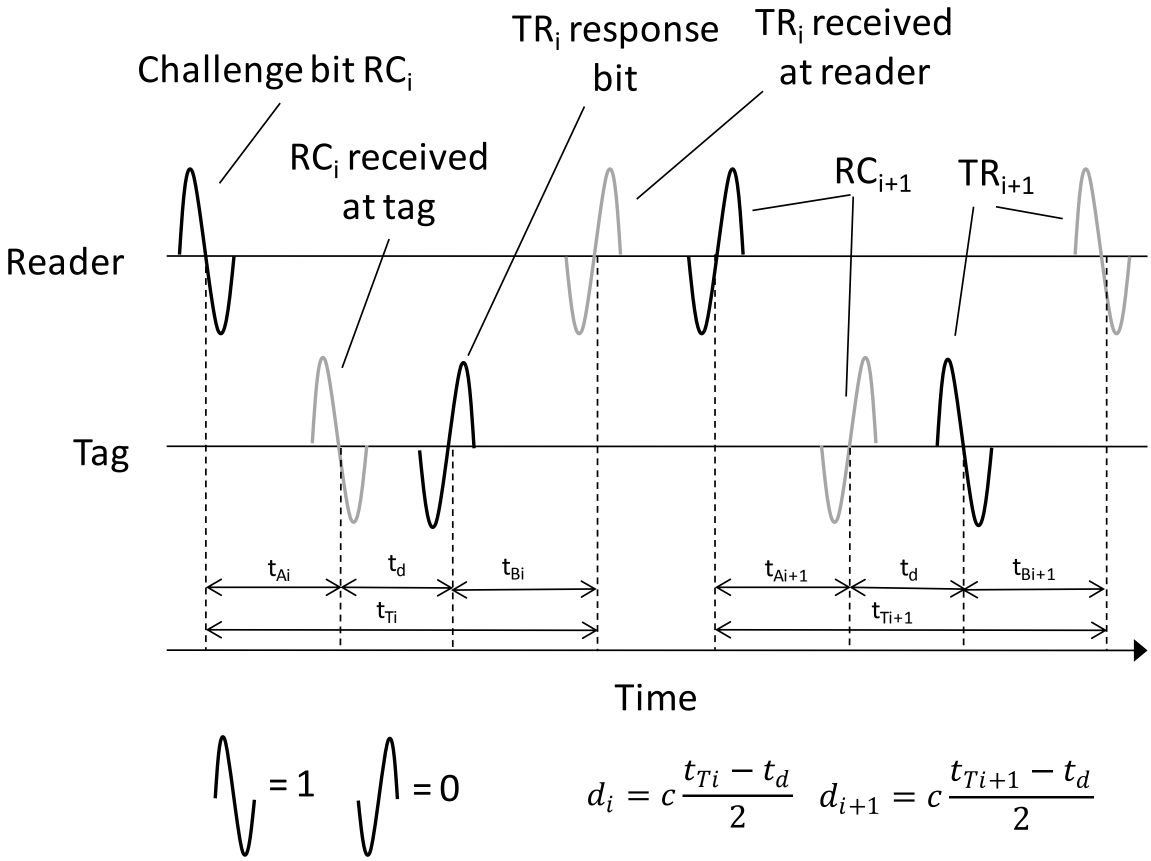
IV. ORNL LOCATION AUTHENTICATION

ORNL is developing a location authentication system to address the issue of location-based attacks. A modified version of a protocol originally introduced by L. Bussard that utilizes a rapid bit exchange for distance bounding is being implemented [4]. The ORNL rapid bit exchange protocol includes cryptographic authentication to ensure identity. Both distance bounding and authentication are intermingled in the same rapid bit exchange to ensure that the same party is executing both elements of authentication.

Ultra-wideband (UWB) is utilized as the physical layer for wireless communications. UWB utilizes short-time-duration pulses for communication, which results in the energy being spread over a large frequency band. The use of short pulses with low duty cycle also results in low overall power consumption. UWB has a number of advantages for safeguards applications including low power operation, immunity to multipath interference, and resistance to jamming. UWB modulation techniques also provide robust transmission signals for accurate time of flight measurement due to the short pulse duration and sharp edges in the time domain signal, making them useful for the accurate RTOF measurements required by the distance bounding protocol.

The ORNL rapid bit exchange protocol between a UWB reader and UWB tag can be seen in Figure 4. Prior to the rapid bit exchange, the reader transmits a random number to the tag. The random number is used to generate a secret message string via a cryptographic method that the reader and tag share. This secret message is divided into a set of challenge bits and corresponding response bits. Each bit exchange begins with the transmission of a challenge bit by the reader. When the tag receives the challenge bit, it is compared with the correct challenge bit previously calculated by the tag. If the challenge bits match, the tag transmits the corresponding response bit. The reader measures the time from the transmission of the challenge bit to the reception of the response bit in order to calculate the distance bound and compares the response bit with the expected response bit to ensure the authenticity of the tag.

The processing delay between the time the tag receives the challenge bit and the time it transmits the response bit adds to the RTOF. If the processing delay is stable, it can be subtracted from the RTOF before calculation of the distance bound, as shown in the equation in Figure 4. Uncertainty in the delay will result directly in uncertainty in the distance bound. Methods for an attacker to manipulate the processing delay may exist, so a more conservative approach would be to minimize the processing delay such that it is insignificant to the final distance bound. ORNL is taking this approach in the system development by eliminating digital processing from the critical path and shortening the delay time to the greatest extent possible in the RF front-end hardware of the tag.



$$d_i = c\frac{t_{Ti} - t_d}{2} \quad d_{i+1} = c\frac{t_{Ti+1} - t_d}{2}$$

Figure 4: ORNL rapid bit exchange.

V. POTENTIAL APPLICATIONS

Secure wireless tagging and tracking is a potential unattended monitoring technology that may meet a number of needs for more efficient and more continuous CoK information. Applications include item identification for use with other unattended monitoring systems, real-time location awareness of items, and continuous tracking of material movements both within and between facilities for comparison to declarations. Use of this technology could increase confidence in CoK, thus reducing the need for physical inspections. It would also provide more timely information on potential diversion activities, increase inspector efficiency during physical inspections via automated data entry and item location awareness, and reduce long-term costs by allowing a greater reliance on CoK and less dependence on physical inspections.

VI. CONCLUSION

There is a need in international safeguards for an effective, secure wireless tagging and tracking technology. Tagging and tracking is a potential unattended monitoring technology that can help the IAEA more efficiently meet the expanding needs for CoK. For location information to be used for verification purposes, a number of potential attack scenarios must be addressed. Location-based attacks are an often-overlooked threat that bypasses typical cryptographic authentication. Distance bounding is a potential solution for detecting location-based attacks, and ORNL has developed an approach utilizing a rapid bit exchange protocol that combines distance bounding with cryptographic authentication.

REFERENCES

1. Dang Nguyen Duc, Hyunrok Lee, D.M. Konidala, Kwangjo Kim, "Open issues in RFID security," Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for Internet Technology and Secured Transactions, pp. 1–5, 9–12 November 2009.
2. S. Brands, D. Chaum, "Distance-Bounding Protocols," *Advances in Cryptology EUROCRYPT '93*, Springer-Verlag LNCS 765, 1993, pp. 344–359.
3. G. Hancke, M. Kuhn, "An RFID Distance Bounding Protocol," *SECURECOMM*, 2005, pp. 67–73.
4. L. Bussard, "Trust Establishment Protocols for Communication Devices," Ph.D. Dissertation, ENST Paris, October 2004, 233 pages.