Facing man-in-the-middle and route diversion attacks in energy-limited RFID systems based on mobile readers

Laura Galluccio, Giacomo Morabito, and Marco Catania
Dipartimento di Ingegneria Elettrica Elettronica e Informatica
University of Catania
Catania, Italy, 95125
Email: first_name.last_name@dieei.unict.it

***Abstract*—Focus of this paper is a large RFID system, where mobile readers detect the presence of RFID tags in the surrounding and, periodically, report the outcome of such operation to a *control center* interested in localizing all RFID tags. In order to deliver the above reports to the control center, mobile readers establish a mobile ad hoc network. In this context, a possible objective of an attacker may be to make the system believe that the position of a certain RFID tag is different from the actual one. To achieve this, the attacker performs man-in-the-middle and routing diversion attacks. Solutions can be devised for combating such attacks but they involve increased energy consumption. In this paper the problem is stated and the tradeoff between security and energy efficiency discussed. Furthermore, some preliminary results are shown and analyzed.**

I. Introduction

The emerging paradigm of the Internet of Things (IoT) is deemed to progressively spread out and realize the vision of pervasive and ubiquitous computing systems [2]. Radio-Frequency Identification (RFID) systems are a significant component of the IoT together with sensors, actuators, mobile phones, etc., which identify objects populating the environment around us. RFID is a promising technology in several application scenarios such as logistics and transportation, documents storage and smart office, thanks to the low costs and implementation simplicity. However, RFID systems have severe security and privacy problems [4], [12] mainly related to the fact that devices spend the majority of the time unattended and so they are more prone to physical attacks. Also eavesdropping can be easily accomplished because of the broadcast nature of the wireless medium. Finally, due to their simplicity, size and limited batteries, RFID tags cannot implement complex cryptographic algorithms and this further limits their security and privacy performance.

More in detail, the main security problems are related to authentication and data integrity. The former is due to the lack of authentication servers which cannot be used in RFID systems because the employed tags are usually passively fed and thus the energy consumed (also associated to exchanged packets) should be reduced as much as possible. Data integrity in RFID systems is also difficult to ensure. In fact data can be modified by adversaries both when stored at the node and when traversing the network [10].

Another very important security problem that has not yet been solved is the *man-in-the-middle* (MiM) attack also called *proxy attack*. Objective of the MiM attack is to let the system believe that a certain tag is located in a position where it is not.

We will focus on the latter kind of attacks in a very challenging scenario, that is when the RFID system is deployed in a large area and readers are mobile nodes and create a mobile ad hoc network. In this context also routing diversion attacks can be performed to deceive the system. Also in this case the proposed solutions should be energy efficient taking into account that readers are likely to be battery powered.

Accordingly, in this paper we will investigate the above types of attacks and the related countermeasures taking into account energy efficiency, besides the effectiveness of the security solutions, as major important metrics. A set of protocols will be identified from the existing literature and some preliminary results will be reported about the tradeoff between security and energy efficiency.

The rest of this paper is organized as follows. In Section II we describe the system model, while the attack model is provided in Section III. The countermeasure we consider are described in Section IV and their performance is evaluated in Section V. Finally, after a survey of the relevant state of the art given in Section VI, we draw our conclusions in Section VII.

II. System model

In this section we describe the model of the system which will be investigated in this paper. More specifically, in Section II-A we provide a description of the networking environment we will consider, while in Section II-B we will provide the models of the RFID reader and tag structures and behaviors.

A. Network model

We consider a RFID system spread over a large area, which we denote as the *network area*. The area is connected to the rest of the infrastructure by means of a gateway, n_0[1]. We

[1]Extension to the general case in which there are several gateways is trivial.

978-1-4577-0899-2/11/$26.00 ©2011 IEEE

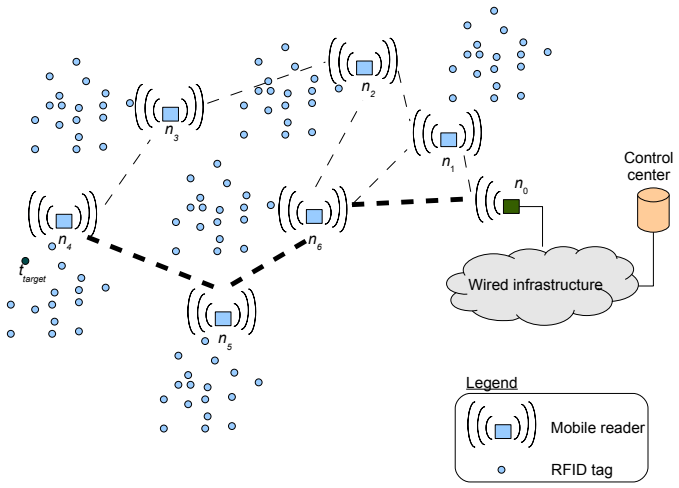

Fig. 1. Exemplary system model.

assume that the address/position of the gateway is known to all nodes in the network.

In the network area, a certain number, N_R, of mobile RFID readers are deployed. We identify the i-th of such readers as n_i, with $1 \leq i \leq N_R$. Such readers have a wireless interface that can be used to communicate with the gateway n_0 that provides access to the rest of the infrastructure.

We assume, however, that the radio coverage of the gateway is not sufficient to provide coverage over the entire network area. Accordingly, the readers form a *mobile ad hoc network* and therefore packets reach their destination according to a multihop wireless communication paradigm. A routing protocol is employed that is able to build and maintain routing tables updated at each node.

Periodically readers query the surroundings to discover the available RFIDs and send a report to a *control center* (which is reached through the gateway). To query the surrounding available tags, the reader transmits a tone at frequency $f_C = 13.56$ MHz [11]. The transmitted power, P_T, is set in such a way that the expected SNR of the signals transmitted by tags within a safety area is higher than the sensitivity of the receiver.

We assume that RFIDs are standard tags with elementary features: they are activated by the signal sent by the reader and modulate the reflection of such signal so as to impress their identifier. We denote the j-th RFID tag (with $j \leq N_T$, where N_T represents the overall number of tags deployed in the network area) as t_j.

For example in Figure 1 we show an exemplary system model. We have that the gateway n_0 provides access to a wired infrastructure to $N_R = 6$ mobile readers. Let us focus on the RFID tag t_{Target} which is located in the proximity of the mobile reader n_4. This mobile reader periodically reports the presence of the RFID tag t_{Target} to the Control Center. To this purpose it will generate messages that will reach the gateway n_0 through the path consisting of the following nodes $\{n_4, n_5, n_6, n_0\}$ (the corresponding links are marked with bold lines).

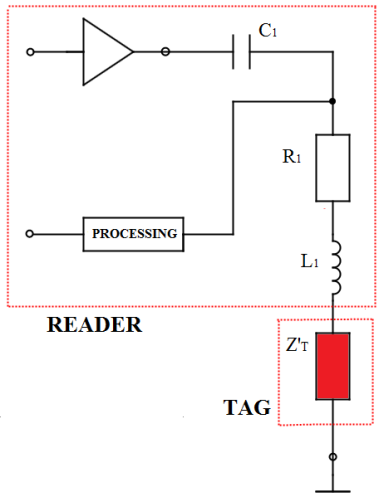

Fig. 2. Equivalent circuit of the Reader-Tag system.

B. Reader/Tag Model

In order to test the resilience of the system to MiM attacks we considered a pair of devices, a reader and a passive tag with inductive coupling. This device is fed by the energy provided by the electromagnetic field generated by the reader. The latter in fact transmits a signal with a carrier f_R around 13.56 MHz. The equivalent coupled system of the reader and the tag is shown in the following Figure 2.

The equivalent circuit seen by the reader consists of

- L_1 which accounts for the inductive effects of the circuit generating the variable magnetic field;
- R_1 which takes into consideration the resistive effects on the reader

- C_1 which accounts for the capacitive effects

When the transponder of tag enters in the variable magnetic field generated by the reader, a current is produced due to inductive coupling on the tag. This coupling effect can be described by means of a virtual impedance Z'_T. The value of Z'_T depends on the operating frequency f and other parameters L_2, R_2, R_L, k and C_2 which are described in [11]. More specifically,

$$Z'_T = \frac{w^2 k^2 L_1 L_2}{R_2 + jwL_2 + \frac{R_L}{1+jwR_L C_2}} \quad (1)$$

This virtual impedance in the equivalent circuit of the reader allows to model the presence or absence of the tag.

To transmit data from the tag to the reader, the load modulation is used. To this purpose a variation in circuit parameters at the tag together with the appropriate sequence of data to be transmitted leads to a modification in Z'_T. This in particular leads to a resistive load modulation which makes the impedance Z'_T switch from a maximum value R_L to a minimum value given by the parallel between R_L and R_{mod}. The latter is a resistive contribution put in parallel to R_L.

The digital sequence that the tag should transmit (i.e. its ID) BPSK modulates a carrier at a frequency sub-multiple of f_R, i.e. $f_T = f_R/\psi$ where for example $\psi = 5$. This signal then causes a load modulation at the reader. In such a way, the modulated signal has a spectrum characterized by two lateral bands which are f_T far away from the f_R.

III. Attack model

Suppose that a certain RFID tag, t_{Target}, is in the area covered by the reader n_{Actual}.

Objective of the attacker is to make the system believe that t_{Target} is in the area covered by another reader, say n_{False}, where, obviously $n_{\text{False}} \neq n_{\text{Attack}}$[2]. Observe that this kind of attacks can be performed when the presence of a tag is related to the possibility to access restricted areas.

To achieve the above objective, on the one hand the attacker needs to convince n_{False} that t_{Target} is within its reach. On the other hand, it needs to prevent n_{Actual} from reporting the presence of t_{Target} within its radio coverage to the control center. In fact, the control center may become alarmed if it detects two readers located far from each other that report the presence of the same tag within their own proximity.

Accordingly, the attacker performs two actions:

- *Man-in-the-middle-attack:* The result of such attack is that the reader n_{False} believes that the RFID tag t_{Target} is in its proximity. To achieve such objective the attacker deploys two nodes, say a_1 and a_2. One of them, say a_1, called *leech*, is deployed close to the RFID tag t_{Target}; the other, i.e. a_2, called *ghost*, is deployed close to the reader that must be deceived, n_{False}. The attacker's node a_2 forwards to a_1 the signals sent by the reader n_{False}, without trying to identify the content of such corresponding messages. The other attacker's node a_1 transmits such signal to t_{Target}, which replies providing its identity (appropriately encrypted). Node a_1 retransmits such reply to a_2 which transmits it towards the reader n_{False}.
  For example, in Figure 3 - which represents the same scenario depicted in Figure 1 - we show how a_1 and a_2 should be deployed to perform man-in-the-middle attack in such a way that the control center believes that the RFID tag t_{Target} is near n_2 and not n_4.
- *Routing diversion attack:* The result of such attack is that the packets transmitted by the mobile reader n_{Actual} should not arrive to the gateway n_0. To achieve such objective the attacker uses the node a_1 which is located near t_{Target} and therefore near n_{Actual}[3]. Node a_1 presents itself as one of the nodes in the ad hoc network and provides fake routing information in such a way that node n_{Actual} considers a_1 as its next hop towards the gateway. Obviously node a_1 will not forward packets received by node n_{Actual} so that true information on target is not received by the control center.
  For example, in Figure 3 node a_1 intercepts the packets transmitted by n_4 but does not forward them towards the gateway n_0.

IV. Countermeasures

In this section we describe possible countermeasures to the above attacks and analyze their cost. More specifically, in Section IV-A we will focus on the man-in-the-middle attack, whereas in Section IV-B we will focus our attention on a possible approach to face the routing diversion attack.

A. Solution to Man in the middle attacks

In Section VI we will describe the approaches proposed so far in the literature to cope with man-in-the-middle attacks in RFID systems. One of the most promising approaches consists in adding a disturbing signal to the tone generated by the reader. The reader will then modulate a disturbed signal which can be demodulated and interpreted only by the reader that introduced it.

Furthermore, note that, if the disturbing signal has the same statistical characteristics of noise then, it will be very difficult for the attacker even to recognize that some message exchange is occurring between the reader and the tag.

However, generation of pseudonoise is very costly as noise power spectral density extends over a very large interval of frequencies. Accordingly, we propose a different approach. Let $c(t)$ represent the tone that would be generated by a given mobile reader, n^*, according to the standard and let $c^{(\text{Modulated})}(t)$ represent the signal that would be transmitted by modulating the tone with a pseudorandom sequence of bits

[2]Observe that n_{False} is not a reader owned by the malicious attacker. It is assumed to be a trusted reader but not the actual one in which coverage area the target tag t_{target} is located.

[3]Note, however that the attacker can achieve the same result by exploiting a third node a_3 located close to any mobile node included in the shortest path between n_{Actual} and the gateway n_0.

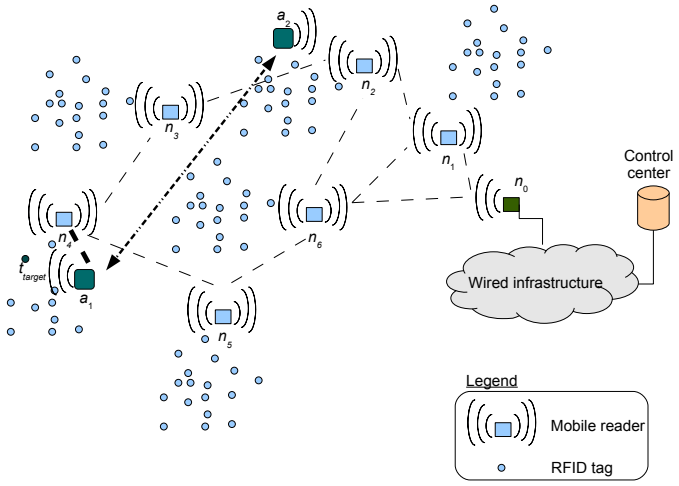

Fig. 3. Examples of the attacks performed to make the control center believe that the RFID tag t_{Target} is in the proximity of n_2.

known to node n^* only. Then the mobile reader node will transmit the signal:

$$c^*(t) = c(t) + c^{(\text{Modulated})}(t) \tag{2}$$

A certain tag t^* which receives such signal will modulate it depending on the data it wants to transfer. Let $x^*(t)$ be the result of such modulation. The reader that receives $x^*(t)$ will subtract $c^{(\text{Modulated})}(t)$ (appropriately attenuated) and then will demodulate the resulting signal. We call such signal $x(t)$, where obviously $x(t) = x^*(t) - A \cdot c^{(\text{Modulated})}(t)$ Performance results show that this operation provides very good performance in terms of decrease in the bit error rate.

Now let us analyze what happens if the man-in-the-middle attack is performed in the same situation. Node a_2 will send the signal $c^*(t)$, generated by node n_{False} to node a_1 which will transmit it. The target RFID tag t_{Target} will reply and such reply will be forwarded by a_1 to a_2, which will transmit it to n_{False}. Suppose that the delay introduced for the transmission of the signal from a_2 and a_1 and viceversa is τ, it is obvious that n_{False} will subtract $c^{(\text{Modulated})}(t)$ from a delayed copy of $c^*(t)$ and therefore, the quality of the received signals will decrease dramatically and the bit error rate will become higher.

B. Routing diversion

The routing diversion problem has been extensively studied in the ad hoc networking literature and several solutions have been devised. The solutions providing an optimal tradeoff between effectiveness in coping with the routing diversion attack and energy efficiency are the following:

- *Mobile reader authentication*: This prevents malicious nodes to pretend they are trusted nodes that can perform message forwarding. Although strong authentication protocols are available in the literature, such solution is not effective in case the attacker achieves control of a *trusted node*.
- *Random routing*: Some randomness is introduced in the selection of the next relay. Accordingly, malicious nodes have difficulties in capturing all packets transmitted by the actual mobile reader n_{Actual}. This type of solutions, however, involve longer end-to-end paths and therefore, larger energy consumption.

In this paper we focus on random routing solutions because their realization is simple. The proposed protocol is basically the same analyzed in [1]. To explain its operations, let n_{CR} represent the current relay, $\Phi\{n_{CR}\}$ represents the nodes within the radio coverage of n_{CR}, and n_{SP} represents the node in $\Phi\{n_{CR}\}$ which is in the shortest path between n_{CR} and the gateway n_0. The basic idea of the random routing algorithm considered in this paper is very simple as it defines the following two phases:

1) Basic parameter of the first phase is the probability p^*. In fact, the current relay n_{CR} immediately selects n_{SP}, which represents the node in the shortest path towards the gateway n_0, as the next relay with probability p^*. If this occurs, then the algorithm stops here, otherwise, it executes the second phase.
2) In the second phase, the current relay n_{CR} randomly selects any of the nodes in $\Phi\{n_{CR}\}$ as next relay.

Note that according to such algorithm n_{CR} selects n_{SP}, that is the node in the shortest path towards the gateway, with probability

$$P_{SP} = p^* + (1 - p^*)/|\Phi\{n_{CR}\}| \tag{3}$$

where $|\Phi\{n_{CR}\}|$ is the number of neighbor nodes of n_{CR}; whereas any given node belonging to $\Phi\{n_{CR}\} - \{n_{SP}\}$ is selected with probability $(1 - p*)/|\Phi\{n_{CR}\}|$.

Note that, the higher p^*, the higher the probability that packets will follow the shortest path, and, viceversa. Accordingly, on the one hand, if p^* decreases we expect longer end-to-end routes between packets source and the gateway n_0 and therefore larger energy consumption. However, on the other hand when p^* becomes smaller, it is more difficult for the

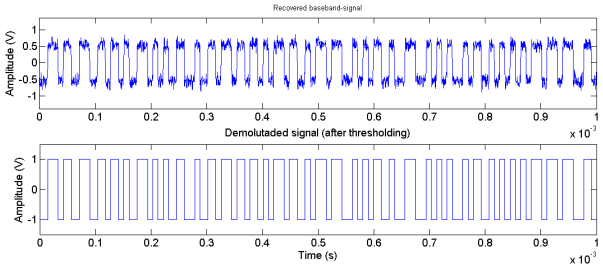

Fig. 4. Upper plot) Signal $x(t)$ obtained at the actual reader n_{Actual}; Bottom plot) Reconstructed sequence of bits at the actual reader, n_{Actual}.

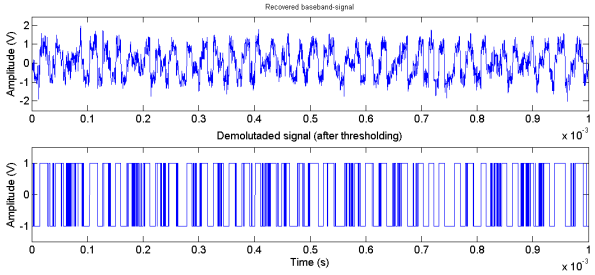

Fig. 5. Upper plot) Signal $x(t)$ obtained at the false reader n_{False}; Bottom plot) Reconstructed sequence of bits at the false reader, n_{False}.

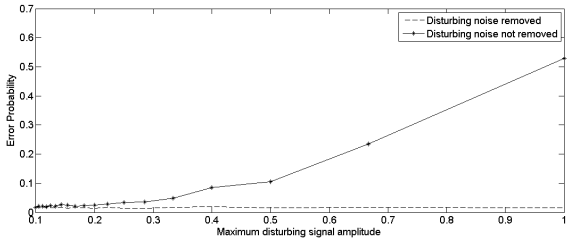

Fig. 6. Bit error probability versus the normalized amplitude of the disturbing signal $c^{(\text{Modulated})}(t)$.

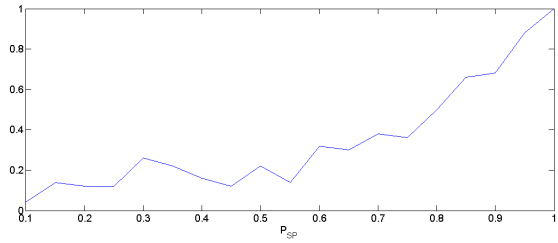

Fig. 7. Percentage of links of the shortest path included in the end-to-end path obtained when random routing is applied versus the probability p^*.

attacker to intercept packets sent by the actual reader of the RFID tag t_{target}, and therefore, the level of security increases.

V. Performance Results

In this section we show the performance results obtained by simulating the countermeasures described in Section IV.

We consider a large RFID system deployed in an area of 1000 x 1000 m^2 where $N_R = 100$ mobile readers are located each with a radio coverage equal to 80 m. We considered an equivalent RFID reader-tag model having the following parameters: $L_1 = 1\mu H$, $C_1 = 137.7pF$, $R_1 = 2.5\Omega$, $Z'_T \in [1.5, 5]k\Omega$, and $f_T = \frac{1}{5} \cdot f_R$. Furthermore, we assume that applying standard RFID protocols the signal-to-noise ratio at the reader receiver block is equal to 40 dB, which gives negligible bit error probability.

In order to evaluate the impact of the countermeasures to the man-in-the-middle attack described in Section IV-A, we compare the output of the reading process in normal conditions and when the man-in-the-middle attack is performed. More specifically, in Figure 4 we give two plots. In the upper plot we show the signal $x(t)$ obtained at the actual reader, n_{Actual}. This is given by the signal modulated by the tag when removed of the disturbance introduced by the reader multiplied by an appropriate constant. In the bottom plot of the same figure, instead, we show the sequence of bits obtained by demodulating the $x(t)$ shown in the upper plot. This is the right sequence generated by the tag.

For the sake of comparison, in Figure 5 we show the same curves obtained at the false reader n_{False} when the man-in-the-middle attack is performed. Note that the sequence of bits obtained after the demodulation is dramatically different, which means that the false reader does not authenticate the target RFID tag t_{Target}. Both Figures 4 and 5 have been obtained by assuming that the amplitude of the disturbing signal, $c^{(\text{Modulated})}(t)$, is 50% of the amplitude of the tone $c(t)$.

To evaluate the impact of the amplitude of the disturbing signal on the performance of the proposed scheme, in Figure 6 we show the bit error rate versus the normalized amplitude of the disturbing signal. Note that when the normalized amplitude reaches the unitary value, bit error probability is 0.5, which means that the man-in-the-middle attack is not effective.

Observe, however, that the increase in energy expenditure goes as the square of the amplitude of the disturbing signal. Accordingly, appropriate tradeoff must be identified to reduce energy consumption .

In order to evaluate the effects of the adoption of random routing in Figure 7 we show the average number of links that are included in both the shortest path and in the path obtained by using random routing versus the value of the probability p^*. Obviously, this value increases as p^* increases and, therefore, the proposed scheme becomes less effective. However, we expect that as p^* increases, the energy consumption decreases. This is indeed demonstrated in Figure 8 where we show the average path length obtained by using random routing versus the value of the probability p^*. Note that as p^* increases, the the average path length decreases and, therefore, energy consumption as well as packet delivery delay decrease.

Note that both Figures 7 and 8 have been obtained by randomly selecting the positions of the source and the destination.

Also in this case we observe that appropriate tradeoff between security and energy consumption should be identified.

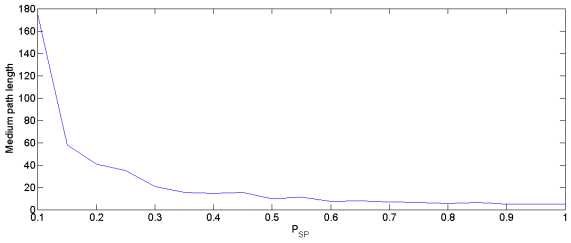

Fig. 8. Average path length obtained by using random routing versus the value of the probability p^*.

VI. Related Work

In this section we will briefly summarize the solutions proposed in the literature to combat the attacks considered in this paper. More specifically, in Section VI-A we will report major countermeasures against man in the middle attacks, whereas, we will focus on routing diversion attacks in Section VI-B.

A. Man-in-the-middle attack

Man-in-the-middle attacks cannot be limited by use of any encryption mechanism performed by RFIDs and readers [12]. Approaches proposed so far to such kind of attack can be classified as follows:

- *Authenticating gestures:* Usually, people execute a certain set of gestures when they want to activate some mechanism utilizing a RFID-enriched card or object. It is unlikely that the same set of gestures are executed by the owner of the target RFID, t_{Target}. Accordingly, it has been proposed (see [16], for example) to deploy accelerometers in the RFID and to train RFIDs so that they learn the sequence of movements performed by their owners when they want the reader to identify them. If RFIDs do not detect the correct sequence of movements, they will remain silent when queried by the reader. This is a very interesting approach, but involves high computational complexity which would require higher computing and energy resources than what is usually available in RFID tags. Also, it applies to certain scenarios only and it is very difficult to generalize it.
- *Bounding reader-tag distance:* Man-in-the-middle attack becomes effective when the distance between the false reader n_{False} and the target RFID tag, t_{Target} becomes large. Accordingly, solutions have been proposed that enforce upperbounds on the maximum distance at which the man-in-the-middle attack can be performed (see [7] and [8], for example). Such solutions are based on an accurate measure performed by the reader on the delay between the time when the query has been transmitted and the time when the reply by the RFID tag is received. If such delay is larger than a given threshold, the reader does not accept the reply. This approach achieves its aim; however, interactions and possible interferences with the MAC anticollisions protocols should be analyzed carefully.
- *Hiding transmissions:* Another interesting approach consists in making the transmissions performed by the reader or the tag indistinguishable from noise. To this purpose (usually) the tag generates a pseudonoise which is modulated by the tag. The authenticated reader will be the only communication node able to interpret the signal transmitted by the tag. Observe that, according to such approach (proposed in [15] and [9], for example), the transmissions of both the reader and the tag have the same statistical characteristics of noise and, therefore, it is impossible for other elements to capture and forward it, which makes the man-in-the-middle attack impossible to perform. Note however, that accurate analysis of the reading range obtained by using standard commercial RFID tag should be performed. Furthermore, it is clear that such kind of solutions require higher transmission power and therefore, cause higher energy consumption.

B. Routing diversion attack

Routing diversion attack in ad hoc networks is a well known security problem that has already received a lot of attention [5]. The most obvious solution to this type of problem could be using flooding to route packets. In this way it is obvious that several copies of the packet will reach the gateway n_0. However,

- It is obvious that energy consumption dramatically increases as well.
- Attacker may introduce packets in the network, so that it is flooded and therefore energy consumption is increased dramatically. In other words such routing protocol makes the network prone to other types of attack that can cause severe problems.

A different approach is called *multipath routing*, as proposed in [14] and [6]. In multipath routing several, say M, (possibly) disjoint paths between the source and the destination are identified. Packets are forwarded throughout all such M paths. Effectiveness of multipath routing against routing diversion increases as the value of M increases. However, large values of M cause large energy consumption as well, and therefore, appropriate tradeoffs should be identified.

A completely different approach consists in detecting nodes that do not retransmit packets that they are expected to forward. Once misbehaving nodes are identified they should be removed by the routing tables of all nodes in the network. This is however a difficult task to accomplish. In fact, if malicious nodes are removed by the routing tables of the nodes that have detected the misbehavior and information about such misbehavior is not propagated, then routing inconsistencies may occur which may create loops in the network. On the contrary, if information about misbehaving nodes is propagated in the network, then solutions should be identified such that malicious nodes are not allowed to cause the exclusion of well behaving nodes from the networks since they can inject false information about misbehavior of good nodes. Examples of such approach can be found in [13] and [3].

Finally, another approach is random routing, which was described in Section IV-B.

VII. Conclusions and future work

In this paper we have focused our attention on a large RFID system consisting of mobile readers that establish a mobile ad hoc network to exchange information with a control center where the position of all RFID tags is reported. More specifically, we have considered an attack aimed at making the system believe that a certain RFID tag is in a position different from the actual one. Such attack will consist in the combination of two well known attacks, namely the man-in-the-middle and the routing diversion attacks. We have identified possible countermeasures to both the above attacks and have discussed their cost in term of increased energy consumption. Furthermore we have provided some preliminary numerical results.

We are now planning to develop a framework for the identification of an appropriate tradeoff between security and energy efficiency. To this purpose we first need to identify which is the lowerbound on the bit error probability that should be encountered by the false reader n_{False} when the man-in-the-middle attack is performed. To this aim it will be necessary to consider the characteristic coding schemes applied in standard RFID transmissions.

Then we need to identify what is the optimal tradeoff between the percentage of packets that can be intercepted by the attacker and energy efficiency.

Acknowledgments

This work was partially supported by the European Commission within the frameworks of the CONVERGENCE project (contract number FP7 - 257123) and the IMSK project (contract number FP7 - 218038).

References

[1] S. Armenia, G. Morabito, and S. Palazzo. Analysis of Location Privacy/Energy Efficiency Tradeoffs in Wireless Sensor Networks. *Proc. of IFIP Networking*. May 2007.

[2] L. Atzori, A. Iera, and G. Morabito. The Internet of Things: A Survey. *Computer Networks*. Vol. 54, No. 15. October 2010.

[3] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens. An on-demand secure routing protocol resilient to Byzantine failures. *Proc. of ACM Workshop on wireless security (WiSe)*. April 2002.

[4] J. Bukley. From RFID to Internet of Things: final report. *Proc. of European Commission Conference*. March 2006.

[5] L. Buttyan and J.-P. Hubaux. Security and cooperation in wireless networks. *Cambridge University Press* 2008.

[6] H. Choi, P. McDanial, and T. F. L. Porta. Privacy preserving communication in manets. *Proc. of 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and networks (SECON)*. June 2007.

[7] K. P. Fishkin, S. Roy, and B. Jiang. Some methods for privacy in RFID communication. *Proc. of 1st European Workshop on Security in Ad-Hoc and Sensor Networks*. August 2004.

[8] G.P. Hancke and M. G. Kuhn. An RFID distance bounding protocol. *Proc. of IEEE/CreateNet Secure Communications*. September 2005.

[9] G. P. Hancke. Modulating a noisy carrier signal for eavesdropping-resistant HF RFID *Elektrotechnik und informationstechnik* Vol. 124, No. 11. 2007.

[10] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, T. Phillips. Guidelines for securing radio frequency identification (RFID) systems. *NIST Special Publication*. April 2007.

[11] ISO/IEC. Information technology – Automatic identification and data capture techniques – Air interface specification for Mobile RFID interrogators. *ISO/IEC 29143:2011*. 2011.

[12] A. Jules. RFID security and privacy: a research survey. *IEEE JSAC* Vol. 24, No. 2. February 2006.

[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. *Proc. of ACM MobiCom*. August 2000.

[14] P. Papadimitratos and Z. Haas. Secure message transmission in mobile ad hoc networks. *Elsevier Ad Hoc Networks*. Vol. 1, No. 1. July 2003.

[15] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert and J. Reverdy. RFID Noisy Reader How to Prevent from Eavesdropping on the Communication? *Springer - LNCS* Vol. 4727/2007. 2

[16] N. Saxena and J. Voris. Still and Silent: Motion Detection for Enhanced RFID Security and Privacy without Changing the Usage Model. *Springer LNCS*. Vol. 6370/2010.