SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2011; **00**:1–12
DOI: 10.1002/sec

RESEARCH ARTICLE

A Context-Aware Approach to Defend Against Unauthorized Reading and Relay Attacks in RFID Systems

Di Ma* and Nitesh Saxena

University of Michigan-Dearborn, Polytechnic Institute of New York University

ABSTRACT

RFID systems are becoming increasingly ubiquitous in both public and private domains. However, due to the inherent weaknesses of underlying wireless radio communications, RFID systems are plagued with a wide variety of security and privacy threats. A large number of these threats arise due to the tag's promiscuous response to any reader requests. This renders sensitive tag information easily subject to *unauthorized reading*. Promiscuous tag response also incites different forms of *relay attacks* whereby a malicious colluding pair, relaying messages between a tag and a reader, can successfully impersonate the tag without actually possessing it. Due to the increasing ubiquity of RFID devices, there is a pressing need for the development of security primitives and protocols to defeat unauthorized reading and relay attacks. However, currently deployed or proposed solutions often fail to satisfy the constraints and requirements of the underlying RFID applications in terms of (one or more of) efficiency, security, and usability.

This paper proposes a novel research direction, one that utilizes sensing technologies, to tackle the problems of unauthorized reading and relay attacks with a goal of reconciling the requirements of efficiency, security, and usability. The premise of the proposed work is based on a current technological advancement that enables many RFID tags with low-cost sensing capabilities. The on-board tag sensors will be used to acquire useful contextual information about the tag's environment (or its owner, or the tag itself). To defend against unauthorized reading and relay attacks, such context information can be leveraged in two ways. First, contextual information can be used to design *context-aware selective unlocking* mechanisms so that tags can selectively respond to reader interrogations and thus minimize the likelihood of unauthorized reading and "ghost-and-leech" relay attacks. Second, contextual information can be used as a basis for *context-aware secure transaction verification* to defend against special types of relay attacks involving malicious readers.

KEYWORDS

RFID, security and privacy, unauthorized reading, relay attack selective unlocking, secure server verification

***Correspondence**

4901 Evergreen Road, Dearborn, MI 48128

Received . . .

1. INTRODUCTION

Low cost, small size, and the ability of allowing computerized identification of objects make Radio Frequency IDentification (RFID) systems increasingly ubiquitous in both public and private domains. Prominent RFID applications include supply chain management (inventory management) [1], e-passports [2], credit cards [3], driver's licenses [4, 5], vehicle systems (toll collection or automobile key) [6–8], access cards (building or parking, public transport) [9], and medical implants [10]. Besides numerous existing applications, RFID is considered as one of the main enabling technologies for the creation of Internet of Things (IoT) - an entirely new network of networks that connects everything, just as how the "traditional" Internet connects everyone. This new Internet paradigm will enable innovative forms of ubiquitous communication between people and things (e.g., physical objects) as well as between things themselves, revolution the way we communicate with our physical environment, and eventually transform the society into a more intelligent one.

A typical RFID system usually consists of tags, readers and/or back-end servers. Tags, also called transponders, are miniaturized wireless radio devices that store information about their corresponding subject. Such information is usually sensitive and personal identifiable. For example, a US e-passport stores the name, nationality, date of birth,

Prepared using secauth.cls [Version: 2010/06/28 v2.00]

digital photograph, and (optionally) fingerprint of its owner [11]. Readers, also known as interrogators, broadcasts queries to tags in their radio transmission ranges for information contained in tags and tags reply with such information. The queried information is then sent to the server (which may co-exist with the reader) for further processing and the processing result is used to perform proper actions (such as updating inventory, opening gate, charging toll or approving payment).

Due to the inherent weaknesses of underlying wireless radio communication, RFID systems are plagued with a wide variety of security and privacy threats [12]. A large number of these threats are due to the tag's promiscuous response to any reader requests. This renders sensitive tag information easily subject to *unauthorized reading* [13]. Information (might simply be a plain identifier) gleaned from a RFID tag can be used to track the owner of the tag, or be utilized to clone the tag so that an adversary can impersonate the tag's owner [12].

Promiscuous response also incites different types of *relay attacks*. One class of these attacks is referred to as "ghost-and-leech" [14]. In this attack, an adversary, called a "ghost," relays the information surreptitiously read from a legitimate RFID tag to a colluding entity known as a "leech." The leech can then relay the received information to a corresponding legitimate reader and vice versa in the other direction. This way a ghost and leech pair can succeed in impersonating a legitimate RFID tag without actually possessing the device. A more severe form of relay attacks, usually against payment cards, is called "reader-and-leech"; it involves a malicious reader using which the owner intends to make a transaction [15]*. In this attack, the malicious reader, serving the role of a ghost and colluding with the leech, can fool the owner of the card into approving a transaction which she did not intend to make (e.g., paying for a diamond purchase made by the adversary while the owner only intending to pay for food). We note that addressing this problem requires *secure transaction verification*, i.e., validation that the tag is indeed authorizing the intended payment amount. The feasibility of executing relay attacks has been demonstrated on many RFID deployments, including the Chip-and-PIN credit card system [15], RFID-assisted voting system [16], and keyless entry and start car key system [6].

With the increasingly ubiquitous deployment of RFID applications, there is a pressing need for the development of security primitives and protocols to defeat unauthorized reading and relay attacks. However, providing security and privacy services for RFID tags presents a unique and formidable set of challenges. The inherent difficulty stems partially from the constraints of RFID tags in terms of computation, memory and power, and partially from the unusual usability requirements imposed by RFID applications (originally geared for automation). Consequently, solutions designed for RFID systems need to satisfy the requirements of the underlying RFID applications in terms of **efficiency, usability** and **security**.

1.1. Existing Countermeasures

Although a flurry of research results have been published, many of them fail to meet the constraints and requirements of the underlying RFID applications in terms of (one or more of) efficiency, security, and usability.

Unauthorized reading could be addressed by means of *selective unlocking* of tags, i.e., tags are made to respond selectively, rather than promiscuously. Hardware-based selective unlocking schemes have been proposed. These include: Blocker Tag [17], RFID Enhancer Proxy [18], and RFID Guardian [19]. All of these approaches, however, require the users to carry an auxiliary device (a blocker tag in [17], and a PDA like special-purpose RFID-enabled device in [18, 19]); such an auxiliary device may not be available at the time of accessing RFID tags, and users may not be willing to carry these devices always. A Faraday cage can also be used to prevent an RFID tag from responding promiscuously by shielding its transmission. However, a special-purpose cage (a foil envelope or a wallet) would be needed and the tag would need to be removed from the cage in order to be read. This greatly decreases the usability of such solutions as users are not willing to put up with changes to traditional usage model given that RFID devices were meant to make life easier for people. Moreover, building a true Faraday Cage that shields all communication is known to be a significant challenge. For example, a crumpled sleeve is shown to be ineffective for shielding purposes [20].

Cryptographic reader-to-tag authentication protocols could also be used to defend against unauthorized reading. However, due to their computational complexity and high bandwidth requirements, many of these protocols are still unworkable even on high-end tags [21]. There has been a growing interest in the research community to design lightweight cryptographic mechanisms (e.g., [22–25]). However, these protocols usually require shared key(s) between tags and readers, which is not an option in many applications.

Distance bounding protocols have been used to thwart relay attacks [6, 15]. A distance bounding protocol is a cryptographic challenge-response authentication protocol which allows the verifier to measure an upper-bound of its distance from the prover [26]. (We stress here that normal "non-distance-bounding" cryptographic authentication protocols have no help in defending against relay attacks.) Using this protocol, a valid RFID reader can verify whether the valid tag is within a close proximity thereby detecting ghost-and-leech and reader-and-leech relay attacks [6, 15]. The upper-bound calculated by an RF distance bounding protocol, however, is very sensitive to processing delay (the time used to generate the response) at the prover side. This is because a slight delay (of the

*In contrast to "ghost-and-leech" attack, the owner in the "reader-and-leech" attack is aware of the interrogation from the malicious reader

Security Comm. Networks 2011; **00**:1–12 © 2011 John Wiley & Sons, Ltd.
DOI: 10.1002/sec
Prepared using secauth.cls

orders of a few nanoseconds) may result in a significant error in distance bounding. Because of this strict delay requirement, even XOR- or comparison-based distance bounding protocols [26,27] are not suitable for RF distance bounding since simply signal conversion and modulation can lead to significant delays. By eliminating the necessity for signal conversion and modulation, a very recent protocol, based on signal reflection and channel selection, achieves a processing time of less than 1 ns at the prover side [28]. However, it requires specialized hardware at the prover side due to the need for channel selection. This renders existing protocols currently infeasible for even high-end RFID tags.

1.2. Our Principles and Approaches

In an attempt to address the drawbacks of prior research, this paper proposes a novel research direction, one that utilizes sensing technologies, to address unauthorized reading and relay attacks in RFID systems. The premise of the proposed work is based on a current technological advancement that enables many RFID tags with low-cost sensing capabilities. Various types of sensors have been incorporated to many RFID tags [29–31]. Intel's Wireless Identification and Sensing Platform (WISP) [32, 33] is a representative example of a sensor-enabled tag which extends RFID beyond simple identification to in-depth sensing. This new generation of RFID devices can facilitate numerous promising applications for ubiquitous sensing and computation [34, 35]. They also suggest new ways of providing security and privacy services by leveraging the unique properties of physical environment or physical status of the tag (or its owner). In this paper, we specifically focus on the design of context-aware security primitives and protocols by utilizing sensing technologies so as to provide improved protection against unauthorized reading and relay attacks.

The physical environment offers a rich set of attributes that are unique in space, time, and to individual objects. These attributes – such as temperature, sound, light, acceleration or magnetic field – reflect either the current condition of a tag's surrounding environment or the condition of the tag (or its owner) itself. A sensor-enabled RFID tag can acquire useful contextual information about its environment (or its owner, or the tag itself). Such contextual information can be leveraged in two ways:

- First, contextual information can be used to design *context-aware selective unlocking* mechanisms so that tags can selectively respond to reader interrogations. That is, rather than responding promiscuously to queries from any readers, a tag can leverage upon "context recognition" and will only communicate when it makes sense to do so, thus raising the bar even for sophisticated adversaries without affecting the RFID usage model, i.e., without imposing additional user burden. For example, an office building access card, equipped with a location sensor, can remain locked unless it is near the (fixed) entrance of the building. The following selective unlocking mechanisms will be explored in Section 2: (i) magnetic-field triggered proximity sensing, (ii) posture recognition, and (iii) location sensing and location classification.
- Second, contextual information can be used as a basis for *context-aware secure transaction verification* to defend against special relay attacks involving malicious readers. For example, a bank server will deny a $2000 transaction when it detects the tag (RFID credit card) is currently located in a restaurant where a normal transaction is usually less than $200. The following two context-aware secure transaction verification schemes will be explored in Section 3: (i) numeric digit-based speech recognition, and (ii) location sensing and location classification

The design of context recognition for RFID tags poses several challenges. First, the resource constraints of RFID tags hamper the complexity of the algorithms that can be used to judge what activity a tag is currently undergoing. Another obstacle is the lack of ways in which users can interact with their tags. RFID tags, being geared for automation, were designed to be as transparent as possible to their users, and as such lack any input or output interfaces such as buttons and displays. Moreover, many users are typically not in direct contact with their tags because they prefer to keep them inside other objects, such as wallets or purses [36]. For example, it is a common practice to swipe one's wallet containing the tag against the reader rather than taking the tag out from the wallet and directly swiping the tag.

1.3. Scope

We note the proposed approach may not provide absolute security due to the possibility of errors associated with context recognition; however, it raises the bar even for sophisticated adversaries without affecting the RFID usage model. In addition, although the proposed techniques can work in a stand-alone fashion, they can also be used with other security mechanisms, such as cryptographic-based schemes, to provide stronger cross-layer security protection according to different security needs in various applications. Moreover, many of the proposed ideas and techniques will be applicable in the realm of other wireless (or wired) devices equipped with sensors. Because sensors serve as a bridge between the physical and the digital world, the proposed sensing-centric mechanisms will be instrumental towards providing dependability, security and privacy for complex Cyber-Physical Systems.

1.4. Economic Constraints

Security comes at a cost. Thus, a fundamental question with respect to our approaches might be: *whether the cost of sensor-enabled tags is acceptable?* The cost of RFID

tags is dependent on several factors such as capabilities of the tag (computation, memory), packaging of the tag (e.g., encased in plastic or embedded in a label), and the volume of tags produced. High-end RFID tags, e.g., those available on e-passports or some of the access cards that are capable of performing certain cryptographic computations like AES or RSA encryption, cost around $5, whereas low-end inventory tags that do not support any (cryptographic) computation cost only about $0.20 [37]. (We emphasize that our proposal generally targets high-end RFID tags that open up a wide array of applications and generally require higher level of security and privacy. Inventory tags, at least for the time being, are not within the scope of our research.) The current cost of WISP tags – equipped with a thermometer and an accelerometer – assembled from discrete components cost roughly $25 but it is expected that this number will be reduced closer to $1 once they are mass manufactured [38]. This cost is certainly acceptable for high-end tags and does not affect their business model. Tag price will not be reduced indefinitely due to the per-die cost for small ICs. Incorporating sensors on tags – i.e., increasing the capabilities of tags – may raise the price of tags initially. However, in the long run, following Moore's law, advances in process technology and mass production should enable tags with more capabilities (such as sensing, increased computation and memory) at the same cost of today's tags [36].

1.5. Power Constraints

Another question we need to answer with respect to the sensing-based approach is: *whether the power drawn from the reader is enough for the tag to perform the proposed tasks?* Since our prototype implementations will be developed on the WISP platform, we discuss the requirements for sensors to work under the power budget of the WISPs, instead of generic RFID tags. WISP is powered by the conversion of induced RF power from the reader into DC voltage (1.8V) in wireless mode [39]. The micro-controller (MCU) MSP430 on the WISP draws approximately 1 mA running at full speed (200 A per MHz). For a sensor to be integratedw with and work on the WISP platform, we have to take into account the following considerations. First, the sensor must allow for a supply voltage of 1.8V [39]. Second, the time and current assumption necessary to make a measurement/sensing (power-on time + settling time) must be small [39]. Third, the power required for additional circuitry essential for interfacing the sensor must be taken into consideration along with the overall power consumed.

A rough approximation of the energy budget available is 1 mA for 1 ms. That is, as long as the product of the current and settling time of the sensor is less than 1mA*1ms, the sensor can be integrated with the WISP and work under the power budget. Otherwise, a storage capacitance has to be added to the WISP to support additional power consumption request [40]. Apparently, not all types of sensor can be supported by the power budget of the WISP. However, low power sensors which meet the above requirements can potentially work within the induced power on the WISP, including those previously implemented on WISP (rectified voltage, light level, temperature, and acceleration). Several recent works have successfully integrated additional sensors on the WISP platform, including capacitive sensor [40], neural sensor [41], and piezo-element (beeper) [42]. Some other sensors that we are interested to explore, and which meet the above requirements include: Honeywell's HMC1053 3-D magnetometer [43], Servoflo Corporation's MS5607 pressure sensor [44], and ST's MP34DB01 audio sensor (microphone) [45].

Besides choosing the appropriate sensors, we also need to design efficient context recognition algorithms so that they can run on the WISP platform. Individual operations can be further optimized to reduce power consumption. As an alternative approach, we can use the checkpoint strategy proposed in [46] to allow a tag to perform demanding computations despite limited energy and interruptions of power that lead to complete loss of the contents of RAM. In short, the idea is for an interrupted tag to backup its RAM state just before it loses power (e.g., when the reader becomes out of range of the tag). When the reader comes in close enough proximity of the tag, the tag can retrieve its backed up state and resume the unfinished operations, without having to re-start them from the very beginning.

1.6. Organization

The rest of the paper is organized as follows. We outline several possible context-aware selective unlocking mechanisms based on conventional sensors (accelerometer, magnetometer, and GPS receiver) in Section 2 where we also discuss research challenges and applications of each mechanism. We describe how to build secure transaction verification schemes based on context recognition in Section 3. We discuss possible attacks targeting sensor-centric solutions and point out necessary further studies in Section 4. Section 5 provides concluding remarks.

2. CONTEXT-AWARE SELECTIVE UNLOCKING

The traditional selective unlocking techniques require special-purpose hardware and/or explicit user involvement (as discussed in Section 1.1); both greatly decrease the usability and acceptability of such solutions. To remedy this, we propose selective unlocking schemes based on context recognition, focusing not only on security and privacy, but also on usability.

Below we first review two recent works on selective unlocking based on context recognition and discuss their merits and dismerits. We next outline possible selective unlocking mechanisms based on conventional sensors such as accelerometer, magnetometer (compass), and location sensors. For each mechanism, we discuss associated design

Security Comm. Networks 2011; **00**:1–12 © 2011 John Wiley & Sons, Ltd.
DOI: 10.1002/sec
Prepared using secauth.cls

challenges and also suggest specific application(s) that could benefit from it.

2.1. Previous Recent Work

"Secret Handshakes" is a recently proposed interesting selective unlocking method that is based on context inference [36]. In order to unlock an *accelerometer-equipped* RFID tag [32, 47] using Secret Handshakes, a user must move or shake the tag (or its container) in a particular pattern. A number of unlocking patterns were studied and shown to exhibit low error rates [36]. A central drawback to Secret Handshakes, however, is that a unique movement pattern is required for each tag to be unlocked. This requires subtle changes to the expected RFID usage model while a standard, insecure RFID setup only requires users to bring their RFID tags within range of a reader.

Keeping in mind the goal of not incorporating any usage model changes, "Motion Detection" [48] has been proposed by us as another selective unlocking scheme. In Motion Detection, a tag would respond only when it is in motion, instead of doing so promiscuously. In other words, if the device is still, it remains silent. This approach hinges on the straightforward observation that accessing a personal mobile RFID tag fundamentally involves moving it in some manner (e.g., swiping an access card in front of the reader). Although Motion Detection does not require any changes to the traditional usage model and raise the bar required for some common attacks to succeed, it is not capable of discerning whether the device in motion is due to a particular gesture or because its owner is in motion. Hence, the *false unlocking* rate of this approach is high, meaning there is a high chance that a tag gets unlocked when it actually should have been locked.

In the following, we outline several new context-aware selective unlocking mechanisms which (1) have both low *false locking* and *false unlocking* rates, and (2) do not necessitate any change to the current usage model.

2.2. Selective Unlocking based on Proximity Sensing

Using this mechanism, a tag gets unlocked whenever it detects it is near a reader. The requirement for tag and reader being near is common in most RFID applications. For example, while making a payment, a user typically needs to bring her contactless credit card (or its container) closer to the reader for transaction processing. This requirement can therefore serve as an effective means to establish a valid context.

One possible way of proximity sensing is through *scalar magnetometers* that measure the total strength of the magnetic field they are subjected to. More specifically, a magnet would be attached to the reader, and when the tag is brought close to the reader, the tag's on-board magnetometer would sense the magnetic field and the tag would get unlocked if the strength of the magnetic field is above some pre-defined threshold. If an adversary intends to unlock a tag, it can simply be in very close proximity of the tag, just like a legitimate reader. However, being near, increases the chances of the adversary being detected. To remain surreptitious, the adversary is therefore forced to generate a stronger magnetic field from an undetectable distance. Our preliminary investigation shows this attack does not seem feasible. Biot Savart's law [49] can be used to predict the strength of the field as follows:

$$\mathbf{B} = \frac{\mu_0 I}{4\pi} \int \frac{d\boldsymbol{\ell} \times \hat{\mathbf{r}}}{r^2} \tag{1}$$

(Here, I is the current flowing through a magnetic source, vector $d\boldsymbol{\ell}$ is the direction of the current, μ_0 is the magnetic constant, r is the distance between the magnetic source and the location at which the magnetic field is being calculated, and $\hat{\mathbf{r}}$ is a unit vector in the direction of $\mathbf{r}$).

In general, Biot Savart's law states that the magnetic field strength decreases inversely proportional to the square of the distance from the location of magnetic source (a current flowing object or a permanent magnet). Hence, it is difficult to control field strength from a distance and magnetic field strength detection can be a promising avenue for proximity sensing.

The size and sensitivity of magnetometers can be very different. For our purpose, a small magnetometer matching the size of an RFID tag with a reasonable level of sensitivity is needed. Tiny, inexpensive atomic magnetometers about the size of a fat grain of rice have been reported [50]. The most sensitive types of atomic magnetometers can detect fields of the order of a femtotesla ($= 10^{-15}$ Tesla) – about one-fifty-billionth the strength of Earth's magnetic field.

We also note that iron and steel can cause shielding effects on magnetic fields. Other materials such as wood, Plexiglas, Styrofoam, brass, copper, aluminum, leather or paper have almost no effect on shielding magnetic fields. This means that a magnetometer can work even when encased in many objects, such as wallets, purses or backpacks. This suggests that a magnetometer-equipped tag would not need to be removed from its container while accessing the tag.

2.3. Selective Unlocking based on Posture Recognition

"Secret Handshakes" described in Section 2.1 is based on gesture recognition. To unlock an accelerometer-enabled tag, a user has to move the tag in a special pattern - gesture. Hence "Secret Handshakes" is obtrusive and requires explicit user involvement, which is not convenient in a frequent use and reduces the usability of such approach.

This motivates the need for study posture recognition to achieve non-obtrusive selective unlocking that does not require user involvement. We liberally use "posture" to denote activities performed by users without special intention but can serve as a valid context in certain applications. One class of such applications involves implanted medical devices (IMDs). Under legitimate IMD access, we can assume that the patient is lying down

on his or her back. Thus, access to the IMD will be granted only when the patient's body is such a pre-defined unique posture. This will prevent an attacker from controlling the IMD in many common scenarios, such as while standing just behind the patient in public. Since posture formations are human activities performed by users unconsciously, posture recognition can provide a finer-grained non-obtrusive unlocking mechanism without purposeful or conscious user involvement.

Posture recognition is similar to gesture recognition to a certain extent. Similar to the gesture recognition Schemes (like the Secret Handshakes scheme [36] we discussed previously), in a posture recognition scheme, user movement can be recorded by motion sensors such as accelerometers and the captured motion data is then compared with a reference posture template which has been recorded by performing the corresponding movement in a reference coordinate system. A match between the captured data and the reference template implies that the user has exhibited a certain posture transition defined by the reference template. However, there is one primary difference between gesture recognition and posture transition recognition, i.e., device tilt. In (hand) gesture recognition systems, users are assumed to be aware of their hand activities. So gestures are performed in a more-or-less controlled way without tilting the tag so that the effect of tilt can be greatly minimized or ignored. However, in posture transition recognition, as we do not require any explicit user involvement, the tag, placed inside a human body in the form of an IMD or into the pockets in the form of a car key, can be tilted due to the movement of human body or the device positioning itself. The reference template is usually collected in a reference coordinate system. However, once a device is tilted, movement data collected from the device is no longer in the reference coordinate system and the corresponding posture will not be detected correctly. It is therefore critical to detect the tag's orientation in order to rotate the data vector back to the reference coordinate system for correct recognition.

Current systems for full orientation estimation, such as the one in Apple iPad2, usually use a set of sensor modalities – typically including gyroscopes, accelerometers and magnetometers – to estimate device orientation. Gyroscopes are used to determine accurately angular changes while the other sensors are used to compensate the integration drift of the gyroscopes and keep this estimate drift free. However, a typical gyroscope requires about $5 \sim 10$ times more power than magnetometer and accelerometer together. Moreover, its comparably larger form factor also makes gyroscope not commonly available in a tiny single package MEMS chip. Considering the resource constrained RFID platforms, it might be necessary to restrict from using gyroscopes, and instead focus on using accelerometers and/or magnetometers for device orientation and posture estimation. As integrated accelerometers and magnetometers are commercially available in tiny packages, an RFID tag with such sensors can be flat and less obtrusive for the user, which makes them very attractive to be used in IMDs or smart car keys. There exist several attempts to use either accelerometers or magnetometers, however, it has been shown that neither of the two sensors is good enough *alone* to estimate full orientation. On the other hand, orientation estimation schemes that use both accelerometers and magnetometers show very promising results [51, 52]. Further study is needed to check whether these schemes (based on both accelerometer and magnetometer) are efficient enough to be applied on the RFID platform.

2.4. Selective Unlocking based on Location Sensing and Location Classification

We notice in quite some applications, (under normal circumstances,) tags only communicate to readers at some specific locations. For example, an access card to an office building needs to only respond to reader queries when it is near the entrance of the building; a credit card should only work in authorized retail stores (which may be located all over the world); toll cards usually only communicate with toll readers in certain fixed locations and when the car travels at certain speed. Hence, location can serve as a good means to establish a valid context. That is, a tag is unlocked only when it is in an appropriate (pre-specified) location. It is suitable for applications where reader location is fixed and well-known in advance.

Location information can be easily obtained through GPS sensors. A new tag from Numerex and Savi Technology has been equipped with GPS sensors and has the ability to conduct satellite communications [53]. Researchers in Oak Ridge National Laboratory also worked with RFID system suppliers in developing new tags by combining GPS and environmental sensors [54]. These tags are designed to track goods anywhere within a global supply chain.

A prerequisite in a location-aware selective unlocking scheme is that a tag needs to store a list of legitimate locations beforehand. Upon each interrogation from a reader, the tag gets its current location information from its on-board GPS sensor and compares it with the list of legitimate locations and decides whether to switch to the unlocked state or not. Due to limited on-board storage (WISP has a 8KB of flash memory) and passive nature of tags, the list of legitimate locations should be kept short. Otherwise, testing whether the current location is within the legitimate list may cause unbearable delay and affect the performance of the underlying access system. Moreover, the list of legitimate locations should not change a lot since otherwise users have to do extra work to securely update the list on their tags. So selective unlocking based on pure location information is more suitable to be used in applications where tags only need to talk with one or a few readers, such as building access cards. It may not be suitable for credit card applications as there is a long list of legitimate retailer stores, store closing and new store opening happen on a frequent basis.

Security Comm. Networks 2011; **00**:1–12 © 2011 John Wiley & Sons, Ltd.
DOI: 10.1002/sec
Prepared using secauth.cls

Selective unlocking based on pure location information presents similar problems when it is applied to RFID toll systems since a toll card needs to store a long list of toll booth locations. We notice vehicles mounted with RFID toll tags are usually required to travel at a certain speed when they approach a toll booth. For example, three out of eight toll lanes on the Port Authority's New Jersey-Staten Island Outer Bridge Crossing permit 25 mph speeds for E-ZPass drivers; the Tappan Zee Bridge toll plaza and New Rochelle plaza, NY has 20mph roll-through speed; Dallas North Toll way has roll-through lanes allowing speeds up to 30 mph. Hence speed can be used as a valid context to design selective unlocking mechanisms for toll cards. That is, a toll card remains in a locked state except when the vehicle is traveling at a designated speed near a toll booth (such as 25-35 mph in the Dallas North Toll Way case). GPS sensors can be used to estimate speed either directly from the instantaneous Doppler-speed or directly from positional data differences and the corresponding time differences [55].

One disadvantage with the GPS-based approach is the reliance on the GPS infrastructure. Thus, selective unlocking would require the constant accessibility of this infrastructure. Another disadvantage is potential delay due to initialization process of GPS receivers. A GPS receiver can have either a cold start or hot start. The hot start occurs when the GPS device remembers its last calculated position and the satellites in view, the almanac (i.e., the information about all the satellites in the constellation) used, the UTC Time, and makes an attempt to lock onto the same satellites and calculate a new position based upon the previous information. This is the quickest GPS lock but it only works if the receiver is generally in the same location as it was when the GPS was last turned off. The cold start is when the GPS device dumps all the information, attempts to locate satellites and then calculates a GPS lock. This takes longer time because there is no known or pre-existing information [56]. The GPS module we are currently experimenting with can normally acquire a fix from a cold start in 35 seconds, and acquire a hot-start fix in less than 2 seconds [57]. For applications which have extremely low delay tolerance, a storage capacitor can be added to the tag in order to help the GPS receiver keep running to avoid cold start [40]. Another disadvantage of the GPS-based approach is that multiple entities may share the same location information, which might not be desirable in some cases. For example, the stores at the same place, but on different levels of a shopping mall, can share the same altitude and latitude information. This motivates the need to design a "localized" approach to location sensing, that does not require any additional infrastructure besides the RFID. One idea is to make use of (multiple) environmental sensors (such as microphone, thermometer, or magnetometer, and perhaps odor and gas sensors) as a means to derive the location-specific information. The intuition is that the "localized data" gathered by these sensors is unique per location (or type of location, such as an office or a hospital), and thus one can build a classifier that can associate this data with a particular location. To justify this, we can consider the example of an access card application. The noise, temperature and odor levels, for instance, and their variations within a certain timeframe, at the office entrance, and at a nearby cafeteria or outside the office building are likely to be quite different. Thus, a classifier can be "trained" to acquire unique features from sensor data gathered at the office entrance building. On every read request (malicious or otherwise), the card will "test" the classifier on current sensor data and get unlocked only on a positive classification instance. Another example is that of an implanted medical tag [42], which will only get unlocked when the classifier detects it to be inside a hospital or a doctor's office, which may possess some unique sensor extracted features.

There exists some prior research which demonstrates the potential for sensor-based location classification [58]. Other prior work also considers wireless radio receivers to address a similar problem [59,60]. A number of challenges need to be addressed in order to realize the RFID location classification approach, however. First, distinct features of environmental data (a "location fingerprint") need to be identified, that remain constant across time, but can be used to uniquely identify a given location (or a location type). Second, a simplistic classifier needs to be developed that can be accommodated within the constrains of an RFID tag; traditional machine learning classifiers may not be feasible due to their high computational requirements. Third, the classifier needs to be robust enough to be used in practice, with low classification errors. The location estimation based approach may not be as fine-grained as the GPS approach. However, we view it as a much simpler alternative, and believe that it can be employed to provide improved security in the face of many common attacks.

3. CONTEXT-AWARE TRANSACTION VERIFICATION

A highly difficult problem arises in situations when the reader, with which the tag (or its user) engages in a transaction, itself is malicious. For example, in the context of an RFID credit card, a malicious reader can fool the user into approving for a transaction whose cost is much more than what she intended to pay. That is, the reader terminal would still display the actual (intended) amount to the user, while the tag will be sent a request for a higher amount. Perhaps more seriously, such a malicious reader can also collude with a leech and can succeed in purchasing an item much costlier than what the user intended to buy [15]. As mentioned in Section 1, addressing this problem requires secure transaction verification, i.e., validation that the tag is indeed authorizing the intended payment amount. Note that selective unlocking is ineffective for this purpose because the tag will anyway be unlocked in the presence of a valid (payment) context.

A display-equipped RFID tag can easily enable secure transaction verification. This, however, necessitates user involvement because (1) the tag must be taken out of one's wallet or purse, and (2) the amount displayed on the tag needs to be validated by the user. Distance bounding protocols have also been suggested as a countermeasure to the reader-and-leech attacks [15]. However, these protocols are currently infeasible (as also reviewed in Section 1.1. In this section, we set out to explore whether sensor-enabled mechanisms can be designed for secure transaction verification.

One possible approach is for the user to indicate to the tag the intended amount of transaction (instead of the tag displaying this to the user, which requires direct access to the tag). Use of touch sensors [31] or on-board buttons is not feasible for this purpose as they would also require direct tag access; buttons will also hamper tag's form factor. Secret Handshakes [36] could be extended though. The user could create numeric patterns depicting the amount by moving her accelerometer-enabled tag (or wallet containing the tag). For example, user can create a '5' and then two '0's up in the air to indicate a transaction worth $500. This method, however, has the same shortcomings as Secret Handshakes – it requires explicit user involvement and has usability implications. Another, potentially more user-friendly, solution is to have the user speak-out the amount of transaction (e.g., digit-by-digit), which the tag can record using an on-board microphone and decode. This method requires some form of numeric speech (digit) recognition.

In order to provide improved resilience, specifically, to reader-and-leech attacks, location sensing could be used. Note that under such attacks, the valid tag and the valid reader would usually not be in close proximity (e.g., the tag is at a restaurant, while the reader is at a jewelery shop [15]). This is unlike normal circumstances whereby the two entities would be at the same location, physically near to each other. Thus, a difference between the locations of the tag and that of the reader would imply the presence of such attacks. Specifically, the tag (credit card) detects its current location and sends this location information encrypted with the key that it pre-shares with its issuing bank; the bank will then compare the tag's location with that of the (jewelery) merchant and reject the transaction if the two mismatch. We note that such a solution can be deployed, with minor changes on the side of the issuer bank, under the current payment infrastructure, where cards share individual keys with their issuer banks (as discussed in [15]). As presented in Section 2, GPS-enabled tags could be used for determining the tag's location. Similarly, the location classification approach described in previous section can also be employed; here the classifier will be executed by the bank's server – not by the tag locally as in selective unlocking – to "test" for tag's location against reader's location. We note that this solution will raise the bar against reader-aided relay attacks because it forces the attacker to be in the same location as the tag's owner in order to be successful.

4. POSSIBLE ATTACKS AND FURTHER STUDIES

In previous sections, we have presented our ideas on how to use various sensing technologies to design new defense mechanisms for enhanced RFID security and privacy. In this section, we tentatively evaluate the security of this sensor-centric approach, discuss potential attacks against it, and point out necessary further studies.

The security of our sensing-enabled defense mechanisms clearly depends on the (in)capability of an adversary to either directly control the sensors or manipulate the environment in which the sensors operate. In our discussion, we assume that tampering or corrupting the tag and its sensors physically is not possible, or can be easily detected. Rather, we concentrate on indirect control of sensors by means of a malicious reader, given that reader is what powers up the sensors. Additionally, we consider malicious manipulation of sensor's environment in order to compromise the security of the underlying mechanism. It is intuitive that tampering with the localized physical environment is a difficult task, for example, when compared with tampering the wireless radio environment (a property which is a foundation for our proposal). At the same time, it is still important to understand the level of security provided by our mechanisms against localized attackers and to identify the mechanisms which remain most resistant in the face of such attackers.

4.1. Manipulation via Malicious Reader

RFID tags and associated sensors are utterly dependent on reader transmissions for energy. A malicious entity who gains control of an RFID reader could thus trivially perform a denial-of-service (DoS) attack by simply refusing to supply enough power for the sensor to operate. Rather than a DoS attacker, in our evaluation, we consider a more clever opponent that may attempt to manipulate onboard tag sensors by subtly adjusting reader parameters. One such attribute is the rate at which a reader issues requests to tags. If an RFID protocol requires that a tag samples its sensor data each time it wakes up, an attacker could manipulate the rate at which samples are taken by changing the frequency at which a reader issues queries. This may have undesirable consequences from a security perspective. Sensor readings taken at different periods may contain more or less entropy, for instance.

Along the same lines, an adversary could modify the signal strength of a RFID reader's transmissions in order to change the amount of power that is made available to tags. Since some tag hardware requires more power to operate than others, this could potentially alter the behavior of sensing hardware. A sensor may not operate correctly, and

Security Comm. Networks 2011; **00**:1–12 © 2011 John Wiley & Sons, Ltd.
DOI: 10.1002/sec
Prepared using secauth.cls

its output may be less accurate or more predictable when it is supplied with less power than its designers intended.

Further studies are needed to understand the impact of manipulations on proposed sensor-centric security solutions via malicious readers.

4.2. Environmental Manipulation

Our mechanisms that are based on sensor data extracted from the environment are subject to environmental manipulation. So whether it is possible for the adversary to control the environment in such a way that compromises the security of the mechanism? We discuss a few possibilities of such an adversarial control vis-a-vis some of our proposed approaches.

First, let us consider the selective unlocking approach based on proximity sensing (Section 2). Here, if an adversary can trigger a sufficiently high-strength magnetic field near the tag, it can unlock the tag without its owner's consent. Clearly, if the adversary can be very close to the tag, it can unlock the tag, just like a legitimate reader, by making use of a simple magnet. However, being in physical proximity of the owner increases the likelihood of detection. Thus, in order to remain clandestine, the adversary must produce a magnetic field of significant strength from a distance. We will conduct an in-depth study exploring the possibility of such attacks. Our preliminary research suggests that it is not possible to induce strong magnetic field from a distance. This is because the magnetic field strength goes down drastically with distance (Equation 1)[†]. This formula suggests that if an attacker wants to generate a field with a strength of, for example, 700 gauss at 20 m away, it would need to generate a field with a strength of roughly $700 * 20^2 = 28$ Tesla at the source (magnet) [1 gauss = 10^{-4} Tesla]. 28 Tesla is a large number, given an MRI's electromagnet is only 3 Tesla. The formula also suggests that it will take a wire carrying a large amount of current (more than 1000 amperes) in order generate a magnetic field strength of just 200 microtesla even from a distance of 1 m. A current of 1000 amperes will be impossible to induce even for a sophisticated attacker (as a reference, a current of about 1 ampere can cause electrocution).

The GPS-based approach relies heavily on the GPS infrastructure and thus may also be prone to the GPS associated vulnerabilities [61–63]. In the context of location-aware selective unlocking or location-aware transaction verification, the adversary can unlock the tag or fool the server if it can feed GPS sensors with the valid location information (office building for an access card, for example). Of existing GPS attack countermeasures [64–66], the one that is mostly suitable to be applied in our RFID sensor setting is the scheme proposed in [66]. This scheme does not require any special hardware and not rely on any cryptography. Instead, a GPS receiver in this scheme uses inertial sensors (i.e., altimeters, odometers, speedometers) and algorithms to measure the discrepancy between its own predicated location and measured location (through received GPS signals) to detect spoofing and replay attacks. It is thus interesting to explore further on whether this sensor-based countermeasure can be seamlessly integrated on a sensor-enabled tag.

In the context of the location classification approach using environmental sensors (Sections 2 and 3), the attacker would need to create environmental data that corresponds to that of a valid location. This may require tinkering with the surrounding temperature, magnetic field or noise, etc. Common sense suggests that doing so would be difficult, if not impossible, without being detected. A detailed investigation will be conducted to rule out any feasible attack vectors that could be exploited even by a sophisticated adversary.

5. DISCUSSION AND CONCLUDING REMARKS

In this paper, we proposed a new research direction to address the issues of unauthorized reading and relay attacks in sensing-enabled RFID systems. The overarching idea was to utilize on-board sensors to provide RFID systems with context-aware intelligence for improved security and privacy awareness. We argued the feasibility of our approach in terms of both technical and economical aspects. We presented our ideas on the design of multiple context-aware selective unlocking mechanisms to prevent unauthorized reading and "ghost-and-leech" attacks. We also showed how secure transaction verification schemes can be built based upon context recognition to defend against "reader-and-leech" relay attacks involving malicious readers. We also discussed potential attacks targeting this sensor-centric approach and pointed out further studies that are needed to fully understand the level of security provided by sensor-centric mechanisms.

We believe that the proposed research direction can have a significant impact on the security and privacy aspects of sensing-enabled RFID systems. Especially, the proposed solutions (once realized), having been designed with the usability requirements of an RFID system in mind, have the potential to be put to use by the general user population. Moreover, although the proposed techniques can work in a stand-alone fashion, they can also be used with other security mechanisms, such as cryptographic-based schemes, to provide stronger cross-layer security protection according to different security needs in various applications.

[†] As a special case of this equation, when the magnetic source is an infinitely long straight wire running a current I, the magnetic field strength decreases inversely proportional to the distance r from the location of magnetic source, i.e., $\mathbf{B} = \frac{\mu_0 I}{2\pi r}$; in another case, when the magnetic source is a permanent magnet or a dipole, the magnetic field strength decreases inversely proportional to the cube of the distance, i.e., $\mathbf{B} = \frac{\mu_0}{4\pi}\frac{2\mu}{r^3}$ (μ is the magnetic moment at the source).

REFERENCES

1. epicorg. Wal-Mart begins tagging and tracking merchandise with RFID. http://epic.org/2010/07/wal-mart-begins-tagging-and-tr.html July 2010.
2. US Department of State. The U.S. electronic passport. Available online at http://travel.state.gov/passport/passport_2498.html.
3. EMVCo. About EMV. Available online at http://www.emvco.com/about_emv.aspx November 2009.
4. Washington State Department of Licensing. Enhanced driver license/ID card. Available online at http://www.dol.wa.gov/about/news/priorities/edl.html.
5. NYS DMV. Enhanced driver licenses and non-driver identification cards. Available online at http://www.nydmv.state.ny.us/broch/C158.pdf July 2010.
6. Francillon A, Danev B, Capkun S. Relay attacks on passive keyless entry and start systems in modern cars. *18th Annual Network and Distributed System Security Symposium (NDSS)*, 2011.
7. ITGlobal Consulting LTD. RFID toll road payment. Available online at http://www.itglobalconsulting.com/rfidtollroadpayment.asp.
8. Infowarscom. Texas Department of Transportation to instate RFID TxTag. Available online at http://www.infowars.com/articles/bb/toll_roads_tx_tag.htm September 2005.
9. RFID Asia. New Ez-Link contactless smart cards converge transit and payment applications. Available online at http://journal.rfid-asia.info/2008/12/new-ez-link-contactless-smart-cards.htm December 2008.
10. Medical News Today. VeriChip corporation announces phase II development of in vivo glucose-sensing RFID microchip with RECEPTORS LLC. Available online at http://www.medicalnewstoday.com/articles/165894.php October 2009.
11. Juels A, Molnar D, Wagner D. Security and privacy issues in E-passports. *Security and Privacy for Emerging Areas in Communications Networks (Securecomm)*, 2005.
12. Juels A. RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications* February 2006; **24**(2):381–394.
13. Heydt-Benjamin TS, Bailey DV, Fu K, Juels A, O'Hare T. Vulnerabilities in first-generation RFID-enabled credit cards. *Financial Cryptography*, 2007.
14. Kfir Z, Wool A. Picking virtual pockets using relay attacks on contactless smartcard. *Security and Privacy for Emerging Areas in Communications Networks (Securecomm)*, 2005.
15. Drimer S, Murdoch SJ. Keep your enemies close:Distance bounding against smartcard relay attacks. *16th USENIX Security Symposium*, 2007.
16. Oren Y, Wool A. Relay attacks on RFID-based electronic voting systems. Cryptology ePrint Archive, Report 2009/422. Available online at http://eprint.iacr.org/2009/422 2009.
17. Juels A, Rivest RL, Szydlo M. The blocker tag: selective blocking of RFID tags for consumer privacy. *ACM Conference on Computer and Communications Security (CCS)*, 2003.
18. Juels A, Syverson PF, Bailey DV. High-power proxies for enhancing RFID privacy and utility. *Privacy Enhancing Technologies*, 2005.
19. Rieback MR, Crispo B, Tanenbaum AS. RFID guardian: A battery-powered mobile device for RFID privacy management. *Australasian Conference on Information Security and Privacy (ACISP)*, 2005.
20. Koscher K, Juels A, Brajkovic V, Kohno T. EPC RFID tag security weaknesses and defenses: passport cards, enhanced drivers licenses, and beyond. *ACM Conference on Computer and Communications Security*, 2009.
21. Juels A. Rfid security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications*, 2006.
22. Juels A, Weis S. Authenticating pervasive devices with human protocols. *International Cryptology Conference (CRYPTO)*, 2005.
23. Bringer J, Chabanne H, Dottax E. HB++: a lightweight authentication protocol secure against some attacks. *Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, 2006.
24. Katz J, Shin J. Parallel and concurrent security of the HB and HB+ protocols. *Advances in Cryptology - EUROCRYPT, International Conference on the Theory and Applications of Cryptographic Techniques*, 2006.
25. Gilbert H, Robshaw M, Seurin Y. HB#: Increasing the security and efficiency of hb+. *Advances in Cryptology - EUROCRYPT, International Conference on the Theory and Applications of Cryptographic Techniques*, 2008.
26. Brands S, Chaum D. Distance-bounding protocols. *Advances in Cryptology - EUROCRYPT, International Conference on the Theory and Applications of Cryptographic Techniques*, 1993.
27. Hancke GP, Kuhn MG. An RFID distance bounding protocol. *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, 2005.
28. Rasmussen KB, Čapkun S. Realization of RF distance bounding. *Proceedings of the USENIX Security Symposium*, 2010.
29. Ruhanen A, et al. Sensor-enabled RFID tag handbook. http://www.bridge-project.eu/data/File/BRIDGE_WP01_RFID_tag_handbook.pdf January 2008.
30. Holleman J, Yeager D, Prasad R, Smith J, Otis B. NeuralWISP: An energy-harvesting wireless neural

DOI: 10.1002/sec
Prepared using secauth.cls

interface with 1-m range. *Biomedical Circuits and Systems Conference (BioCAS)*, 2008.
31. Sample A, Yeager D, J S. A capacitive touch interface for passive RFID tags. *IEEE International Conference on RFID*, 2009.
32. Sample A, Yeager D, Powledge P, Smith J. Design of a passively-powered, programmable sensing platform for UHF RFID systems. *IEEE International Conference on RFID*, 2007.
33. Smith JR, Powledge PS, Roy S, Mamishev A. A wirelessly-powered platform for sensing and computation. *8th International Conference on Ubiquitous Computing (Ubicomp)*, 2006.
34. Buettner M, Greenstein B, Sample A, Smith JR, Wetherall D. Revisiting smart dust with rfid sensor networks. *ACM Workshop on Hot Topics in Networks (Hotnets-VII)*, 2008.
35. Isik MT, Akan OB. Wireless passive sensor networks. *IEEE Communication Magazine* August 2009; **47**(8):92–99.
36. Czeskis A, Koscher K, Smith J, Kohno T. RFIDs and secret handshakes: Defending against Ghost-and-Leech attacks and unauthorized reads with context-aware communications. *ACM Conference on Computer and Communications Security*, 2008.
37. Wagner D. Privacy in pervasive computing: What can technologists do? Invited talk, SECURECOMM 2005. Available online at http://www.cs.berkeley.edu/ daw/talks/SECCOM05.ppt September 2005.
38. Buettner M, Prasad R, Philipose M, Wetherall D. Recognizing Daily Activities with RFID-Based Sensors. *International Conference on Ubiquitous Computing (UbiComp)*, 2009.
39. WISP Wiki. http://wisp.wikispaces.com.
40. Yeager D, Prasad R, Wetherall D, Powledge P, Smith J. Wirelessly-Charged UHF Tags for Sensor Data Collection. *IEEE International Conference on RFID*, 2008.
41. Holleman J, Yeager D, Prasad R, Smith J, Otis B. NeuralWISP: An energy-harvesting wireless neural interface with 1-m range. *BioCAS*, 2008.
42. Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, Fu K, Kohno T, Maisel WH. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. *IEEE Symposium on Security and Privacy*, 2008.
43. Heneywell. 1, 2 and 3 axis magnetic sensors. Available online at http://www51.honeywell.com/aero/common/documents/myaerospacecatalog-documents/Defense_Brochures-documents/HMC_1051-1052-1053_Data_Sheet.pdf.
44. Servoflo Corporation. New micro altimeter ms5607 for barometric pressure measurement. Available online at http://www.servoflo.com/news/295-new-5607-barometric-pressure-sensor.html.
45. STcom. MP34DB01 MEMS audio sensor omnidirectional digital microphone. Available online at http://www.st.com/internet/com/TECHNICAL_RESOURCES/TECHNICAL_LITERATURE/DATASHEET/CD00284650.pdf Apr 2011.
46. Salajegheh M, Clark S, Ransford B, Fu K, Juels A. Cccp: Secure remote storage for computational rfids. *18th USENIX Security Symposium*, 2009; August.
47. Smith JR, Sample AP, Powledge PS, Roy S, Mamishev A. A wirelessly-powered platform for sensing and computation. *Proceedings of Ubicomp 2006*, 2006.
48. Saxena N, Voris J. Still and silent: Motion detection for enhanced rfid security and privacy without changing the usage model. *Workshop on RFID Security (RFIDSec)*, 2010.
49. Griffiths DJ. *Introduction to Electrodynamics (Third Edition)*. Prentice Hall, 1999.
50. Bourzac K. TR10: Atomic magnetometers. Available online at http://www.technologyreview.com/biotech/20239/ April 2008.
51. Huyghe B, Doutreloigne J. 3d orientation tracking based on unscented Kalman filtering of accelerometer and magnetometer data. *IEEE Sensors Application Symposium*, 2009.
52. Yun X, Bachmann ER, McGhee RB. A simplified Quaternion-based algorithm for orientation estimation from earth gravity and magnetic field measurements. *IEEE Tran. on Instrumentation and Measurement* Mar 2008; **57**(3).
53. Goldiron. Numerex unveils hybrid tag includes active RFID, GPS, satellite and sensors. Available online at http://goldiron.wordpress.com/2009/02/25/numerex-unveils-hybrid-tag-includes-active-rfid-gps-satellite-and-sensors/ February 2009.
54. Buckner M, Crutcher R, Moore MR, Smith SF. GPS and sensor-enabled RFID tags. Available online at http://www.ornl.gov/ webworks/cppr/y2001/pres/118169.pdf.
55. Cropsey G. Designing a distance and speed algorithm using the global positioning system. Available online at http://www.egr.msu.edu/classes/ece480/capstone/spring08/group10/doc Note- Gabe.pdf March 2008.
56. GPS Glossory 2011. Available at: http://www.gsmarena.com/glossary.php3?term=gps.
57. 66-Channel LS20031 GPS Receiver Module 2011. Available at: http://www.megachip.ru/pdf/POLOLU/66_CHANNEL.pdf.
58. Wendlandt K, Khider M, Angermann M, Robertson P. Continuous location and direction estimation with multiple sensors using particle filtering. *IEEE International Conference on Multisensor Fusion and*

Integration for Intelligent Systems, 2006.
59. Qiu D, Lo S, Enge P, Boneh D, Peterson B. Geoencryption using Loran. *The Institute of Navigation International Technical Meeting*, 2007.
60. Qiu D, Lo S, Enge P, Boneh D, Peterson B. Robust location tag generation from noisy location data for security applications. *The Institute of Navigation International Technical Meeting*, 2009.
61. Warner JS, Johnston RG. Think GPS cargo tracking = high security? Technical report, Los Alamos National Laboratory 2003.
62. Papadimitratos P, Jovanovic A. Protection and fundamental vulnerability of global navigation satellite systems (GNSS). *International Workshop on Satellite and Space Communications (IWSSC*.
63. Hanlon B, Ledvina B, Psiaki M, Jr PK, Humphreys TE. Assessing the GPS spoofing threat. GPS World, Available online at http://www.gpsworld.com/defense/security-surveillance/assessing-spoofing-threat-3171?page_id=1 January 2009.
64. Scott L. Anti-spoofing and authenticated signal architectures for civil navigation signals. *16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS)*, 2003; 1543–1552.
65. Kuhn M. An asymmetric security mechanism for navigation signals. *6th Information Hiding Workshop*, 2004.
66. Papadimitratos P, Jovanovic A. GNSS-based positioning: Attacks and countermeasures. *IEEE Military Communications Conference (MILCOM)*, San Diego, CA, USA, 2008; 1–7.

DOI: 10.1002/sec
Prepared using secauth.cls