Robust RFID Authentication for Supply Chain Management

Binod Vaidya, Dimitrios Makrakis
Broadband Wireless & Internetworking Research Lab,
School of Electrical Engineering and Computer Science
University of Ottawa
Ottawa, Canada
{bvaidya, dimitris}@eecs.uottawa.ca

Hussein T. Mouftah
School of Electrical Engineering and Computer Science
University of Ottawa
Ottawa, Canada
mouftah@eecs.uottawa.ca

***Abstract*—Radio Frequency Identification (RFID) technology is promising technology in ubiquitous computing area. RFID is used for various applications, ranging from inventory systems to supply chain management solutions such as vehicle fleet management. In supply chain management system, RFID tag is used to identify the object, to which it is attached, without any physical contact in various locations. This makes tags susceptible to information leak. Thus security and privacy issues remain a major issue. Suitability of public key cryptography solutions in RFID system is open research problem. In recent years, practicability of asymmetric cryptography on RFID applications has been discussed. Though EC-GPS scheme allows compact implementation on a tag, it has several flaws. In this paper, we propose robust RFID authentication scheme for supply chain process using improved EC-GPS. We have provided security proof, security analysis and performance evaluation of the proposed scheme to show its robustness.**

Keywords-RFID network; Supply chain management; Authentication; Public key cryptography

I. INTRODUCTION

Radio Frequency Identification (RFID) technology is one of the most promising technologies in the field of pervasive and ubiquitous computing. With the advancement of emerging pervasive and ubiquitous computing, RFID applications are becoming part of our everyday life. RFID is used for a variety of applications, ranging from inventory systems to inclusive supply chain management solutions. For instance, fleet management and vehicle tracking services identify location and direction of movement of each vehicle in a fleet in real-time, and automatically report such information, and status of predetermined events in which the vehicle is engaged, directly to the control center.

In general, RFID systems consist of many RFID tags and RFID readers. While RF tags operate as transponders, RF readers act as transceivers. In supply chain environment, tags are created in large quantities by numerous untrusted parties and their use is relatively uncontrolled.

In supply chain management system, RFID tag (i.e. transponder) is used to identify the object, to which it is attached, without any physical contact in various locations since it can be read from a distance using strength of the electromagnetic (EM) field of the interrogating reader. However, this makes RFID tags susceptible to information leak. Any reader may be able to read information on RFID tag if that tag is close enough to the reader. Thus security and privacy issues remain a major issue in wide spread deployment of RFID based supply chain management networks. Robust authentication mechanism is required for the supply-chain management, as product authentication in supply chain provides enormous opportunities to combat illegal trade.

Suitability of public key cryptography (PKC) solutions in RFID system is an open research problem due to severe restrictions in costs, area and power. However, despite these relatively pessimistic prospects, some researchers have discussed practicability of asymmetric cryptography on RFID-tags applications [2,3,8]. Among PKC-based RFID identification schemes, GPS identification scheme is promising solution, which lets the owner of a secret key to prove possession of that secret by means of an interactive protocol. In the case of RFID deployment, the tag would prove that it contains a tag-specific secret to a reader and the reader is thereby assured that the tag is authentic. Only an object owning the key could provide required responses during interaction with the reader.

Among several variants of GPS identification protocol [2,4], EC-GPS requires less on-tag memory and less power consumption than most symmetric techniques. At the same time, the computational effort for the reader remains reasonable. However, EC-GPS scheme has several severe flaws, including denial of services (DoS) attacks.

In this paper, we propose a robust RFID authentication scheme for the supply chain management, which includes improved EC-GPS. Since the proposed scheme can resist several active attacks including DoS attacks, it is especially appropriate for RFID deployment in an open network environments.

The rest of this paper is organized as follows. In Section II, we present the related works whereas in Section III, we describe RFID in Supply chain management. Section IV describes the proposed RFID authentication scheme for supply chain management, while Section V discusses the system analysis. And finally Section VI concludes the paper.

978-1-4673-1881-5/12/$31.00 ©2012 IEEE

II. RELATED WORKS

In this section, we discuss related works addressing RFID security using public key cryptography (PKC). Particularly, Schnorr-like identification schemes for RFID tag applications will be focused.

Two prominent varieties of PKC based RFID identification protocols can be identified. The first approach, introduced by Shamir [12], relies on a variation of Rabin cryptosystem and replaces squaring of a plaintext with an addition of a random multiple of the divisor. The Rabin cryptosystem-type approach is implemented in SQUASH [12] as well as in WIPR [8].

The second one uses a token-based approach where pre-computed coupons are stored on the tag. The tag, when queried, uses up these coupons to authenticate itself to the reader. The coupons are such that the tag only needs to do a limited number of operations to use them. The coupon-type scheme is RFID-optimized implementation of GPS protocol [9], which is implemented by McLoone and Robshaw [2].

Both approaches contain some advantages and disadvantages. The Rabin cryptosystem-type approaches do not have any limitation on number of authentications, but they are susceptible to several active attacks. On the other hand, even though the coupon-type approach is quite simple, it can be easily rendered useless by a malicious reader through the simple exhaustion of coupons, i.e. DoS attack.

C.P. Schnorr first introduced a concept of identification protocol using a public key algorithm that allows entity authentication using a zero-knowledge proof-of-knowledge, i.e. a second party does not learn anything about used secret [1]. The Schnorr protocol is a well-known protocol whose security properties can be formally proven.

Another Schnorr-like approach was proposed by M. Girault, G. Poupard and J. Stern, which provides faster authentication. GPS identification protocol [2] is a zero-knowledge protocol that allows small hardware implementations of the prover wanting to assure its identity.

There are several variants and optimizations of the GPS protocol [2-7]. A series of optimizations is realized to ease computation and storage costs. The variants of GPS protocol [3] are mainly based on complete (full) coupon, or partial coupon [11], or coupon-re-calculation [4]. Due to the use of coupons, the authentication of the tag can be performed "on-the-fly" during authentication phase. An elliptic curve variant of GPS (EC-GPS) [2] that uses elliptic curve cryptography (ECC) and pre-computed coupons, has smaller keys. Some storage optimization is described in [2,10]. Use of Low Hamming Weight (LHW) challenges [10] can reduce parameter sizes. A combination of coupons with LHW challenge yields best performance profile for implementation in resource-constrained environments.

McLoone and Robshaw replace a modular exponentiation with a coupon and a simple integer (non-modular) calculation [2]. They propose multiple implementations of their scheme, notably with and without a pseudo random generator (PRG) to help re-generate a random number inside the coupon. The PRG takes about 1000 gate equivalences on the tag, but drastically reduces coupon sizes. With the PRG, the implementation fits on no more than an estimated 1500 gate equivalences, and 10 such reduced-sized coupons take up approximately 500 GEs, for a total of 2000 GEs.

In GPS protocol, on-tag computation reduces to a simple integer computation of a response from the tag with a challenge provided by the reader. Since this is a regular integer computation consisting solely of a multiplication and a subtraction, it can be determined why the GPS protocol is preferred in resource-constrained environments.

III. RFID IN SUPPLY CHAIN MANAGEMENT

In this section, we will depict RFID based Supply chain management and possible security solution for it.

A. RFID based Supply Chain Management

A supply chain management involves the flow of materials, information, and finance as they move through supply chain partners such as manufacturers, suppliers, distributors, retailers, and consumers. A prime objective of supply chain management is to increase long-term performance of individual company and overall supply chain by maximizing customer value and minimizing costs. Fig. 1 shows overviews of Supply Chain management.

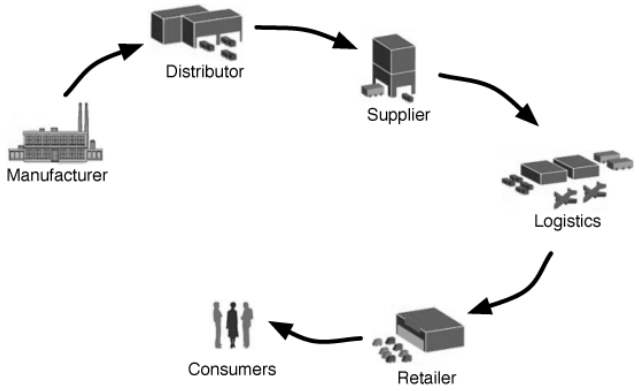

Figure 1. Overviews of Supply Chain Management

In supply chain management system, RFID tag is used to identify the object, to which it is attached, without any physical contact in various locations. RFID can have a significant impact on every aspect of supply chain management from moving goods through loading docks, to managing big data as information about goods collected in real time manner. RFID has potential to dramatically improve supply chain management by reducing costs, inventory levels, stock outs and shrinkage rates; increasing throughput, quality, manufacturing flexibility; and enhancing inventory visibility, inventory record accuracy, customer service, and collaboration among supply chain partners.

B. Security Solution for RFID Supply Chain Management

RFID-enabled supply chain management system is prone to numerous threats and attacks. Typical attacks on tags and readers are impersonation attack, skimming attack,

eavesdropping attack, man-in-the-middle (MiTM) attack, replay attack, denial of service (DoS) attack, and physical attack. RFID tags may be counterfeited in the form of cloned tags on fake products or clone tags on genuine product.

Authenticated supply chain management system is proposed that can deliver robust security solution by using improved EC-GPS to furnish tag authentication as well as using a tag digital signature to ensure that the tag is genuine to a specific manufacturer and is not counterfeit. Due to a space limitation, we will omit a tag digital signature.

IV. IMPROVED EC-GPS SCHEME FOR RFID SYSTEM

In this section, we will propose a robust RFID authentication for the Supply Chain management system. First we will point out several shortcomings of the existing GPS identification protocol. Viewing severe flaws in the existing GPS protocol, we propose improved ECC based GPS identification protocol that is called iEC-GPS.

The notations used to describe the proposed system are shown in Table I.

TABLE I. NOTATIONS USED IN PROPOSED SCHEME

Symbol	Description
E	Elliptic curve
P	Base point
s, V	Secret and public keys of RFID tag
(r_i, X_i)	Coupon
r_i	Witness
α	Commitment
y	Response
$h(.)$	One way hash function

A. GPS protocol and its limitations

In GPS protocol, coupons (r, X) are pre-calculated values that are independent of the input of the verifier. These coupons are stored in the internal memory of RFID tags and are used during an authentication process. After receiving X from a tag, a reader will generate challenge (c) and send it to corresponding tag. With c, r and secret key (s), the tag will compute a response (y) and send it to the reader. Then the reader can verify the received response.

We will point out the shortcomings of GPS protocol. It is susceptible to several of following attacks.

1) Timing attack: A timing attack on GPS identification scheme can recover the prover's private key provided the exponentiation's running time is dependent in the exponent's Hamming weight [5]. While applying this attack, the attacker impersonates the verifier, and is able to measure precisely the computation time for the commitment step. However, one of the countermeasures is to use pre-computed commitments [5].

2) DoS attack: DoS attack is preformed when an adversary wants to make the prover unusable by any means. GPS identification scheme with stored pre-computed coupons is vulnerable to DoS attack since a prover has to utilize its coupon to perform authentication/verification. The number of coupons available is bounded by the memory. As no verifier authentication is required, an adversary can impersonate as a verifier and ask a prover for more verification in a very short period of time. He can exhaust all the coupons almost instantaneously without prover's agreement. The prover will no longer be able to successfully perform the protocol [6]. If GPS scheme is used "without coupons", there will be no DoS attack, however, it will increase computation burden to prover.

3) Stolen coupon attack: A malicious user may illegally acquire stored coupons in a RFID tag to perform following attack. He can learn X, c, and y by eavesdropping continuously traffic flows between the prover and the verifier. Then he can conduct offline computations to resolve corresponding r from the obtained X, and compute s after knowing r, c, and y. Accordingly, the adversary can easily disclose private key s.

B. iEC-GPS protocol

Viewing the existing features as well as above-mentioned weakness of EC-GPS identification protocol, it can be seen that this protocol is not suitable for applications, where recurrent authentication is required. In order to overcome security flaws mentioned above, the variant of GPS identification protocol called iEC-GPS (improved EC-GPS) protocol is proposed in this paper.

ECC is used in the proposed protocol that provides similar security to public key algorithms such as RSA but with smaller key sizes and memory requirements. The principal parameters for ECC are an elliptic curve E defined over a finite field F_q, and a designated point P on E called a base point. The ECC relies on an assumed difficulty of the elliptic curve discrete logarithm problem (ECDLP), which is given points P and $Q=k.P$; it is computationally intractable to determine k.

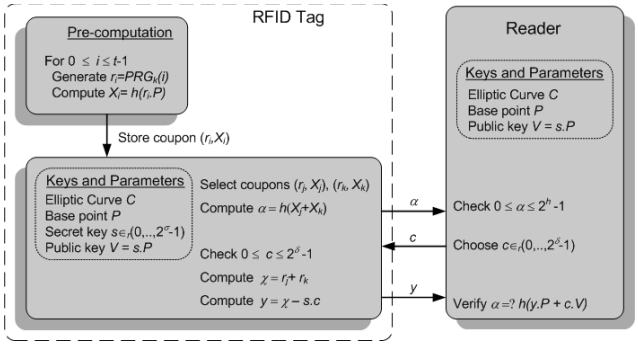

Figure 2. Overview of the iEC-GPS scheme

While the proposed protocol fairly similar to the principle of EC-GPS protocol, there are several fundamental differences. One of the distinguished variations is the computation of commitment and verification of the response.

The pre-computation procedure in iEC-GPS scheme is similar to that of the EC-GPS protocol. That means, a prover can pre-compute a set of coupons off-line and securely store them in the memory for further computation. However, in the

proposed scheme, iEC-GPS scheme, randomly two coupons are used in pair.

The prover selects two coupons (r_j, X_j) and (r_k, X_k) and computes a commitment (α) using the point addition operation and one-way hash function as follows.

$$\alpha = h(X_j + X_k) \quad (1)$$

And after receiving challenge c from the verifier, the prover will compute the response y as follows:

$$\chi = r_j + r_k \quad (2)$$

$$y = \chi - c.s \quad (3)$$

Then the prover (ie tag) will send the response y to the verifier (ie reader). After receiving it, the verifier will verify the result as follows:

$$\alpha =? h(y.P + c.V) \quad (4)$$

In order to guarantee the statistical zero-knowledge property, we will follow the equation $r = c.s.2^{80}$ for the experiments as mentioned in [3,9].

The most significant advantage of the iEC-GPS protocol over EC-GPS protocol is that the prover needs to store only small number of coupons in the memory; yet can generate a large number of commitments.

V. System Analysis

In this section, we provide security proof, security analysis and performance evaluation of the proposed scheme.

A. Security Proof

In order to demonstrate verification of (4), we provide the following security proof.

If (4) holds, the verifier (i.e. reader) shall confirm that the prover (i.e. tag) is genuine.

$$\alpha = h(y.P + c.V)$$

Proof

$$= h((\chi - c.s)P + c.s.P)$$
$$= h(((r_j + r_k) - c.s)P + c.s.P)$$
$$= h(r_j P + r_k P - c.sP + c.s.P)$$
$$= h(r_j P + r_k P)$$
$$= h(X_j + X_k)$$

B. Security Analysis

Numerous attacks such as modification attack, MiTM attack, DoS attack could threaten security of RFID enabled supply chain management network. We will evaluate the proposed iEC-GPS scheme for passive attacks (eavesdropping) and active attacks including impersonation attack, MiTM attack, timing attack, DoS attack and stolen coupon attack.

1) Impersonation attack: If the adversary tries to impersonate a tag, he needs to know private key s and commitments (r_i, r_j) to compute valid response y. Deriving s and (r_i, r_j) are not feasible due the intractability of the ECDLP.

2) MiTM attack: If the attacker can perform MiTM attacks in the RFID supply-chain management network then he has to be capability for capturing and modifying all communication flows between the tag and the reader. However the proposed scheme can resist MiTM attacks since the adversary cannot derive the sensitive information (ie., r_i, r_j, s) from the message flows (ie, α, c, y). Even though he modifies the message flow, it will be detected during verification process with (4).

3) DoS attack: The adversary can perform DoS attack in order to exhaust stored coupons in short period of time. However, in the proposed schemes, since coupons are reusable, commitment is computed such a way that the adversary could not be able to drain the stored coupons.

4) Timing attack: The proposed schemes can resist timing attack as both schemes have set of pre-computed coupons in the memory.

5) Stolen coupon attack: The proposed schemes are capable for resisting stolen coupon attack. Even though the adversary manages to obtain all message flows (α, c, y), he would not be able to derive (r_i, r_j) from the obtained information because the proposed schemes use point addition operation and one-way hash function for the computation of α.

6) Eavesdropping attack: Since the communicating parties have secret session key to encrypt all the communications between them, the proposed schemes can prevent from eavesdropping attacks.

C. Performance Evaluation

In this sub-section we will illustrate the performance evaluation of the proposed scheme.

Initially, we will demonstrate the robustness of the proposed scheme, iEC-GPS. Fig. 3 shows number of coupons versus number of commitments generated in the existing EC-GPS scheme and the proposed iEC-GPS scheme.

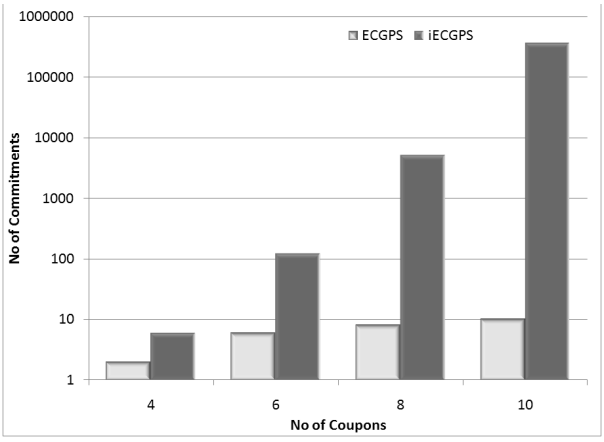

Figure 3. Coupons versus commitments in EC-GPS and iEC-GPS schemes

From Fig. 3, it can be seen that for 10 coupons, the existing EC-GPS scheme has only 10 possible commitments whereas

the proposed iEC-GPS scheme has more than 300,000 possible commitments. The proposed iEC-GPS scheme does not necessitate storing a large number of coupons in the memory. Even with small number of coupons, the large number of commitments can be computed for efficient deployment. Furthermore, frequent re-calculation of the coupons is avoided, which may costly operation.

In cases of the EC-GPS scheme, it is susceptible to DoS attack. If the stored coupons are exhausted, it has to compute new commitment every time when it desires to send authentication request. Computing a commitment is rather costly as it uses point multiplication operation.

Then, we have simulated a straightforward RFID enabled system and compare the proposed scheme with the existing scheme as well.

The main purpose of this performance analysis is to evaluate the effect of DoS attack in the proposed scheme and compare with the existing representative scheme.

For the scenario, we define attack model in which attackers emerge for certain time and intentially deplete the stored coupons in the user during that period of time. We will consider naïve attack model, in which after receiving a response from the tag, the adversary will wait for some time to send a next round of authentication request to the tag as if it is verifying the response.

We have considered authentication success ratio as a performance metric for this scenario. The authentication success ratio is a ratio of authentication requests that are concluded successfully with respect to the total number of requests.

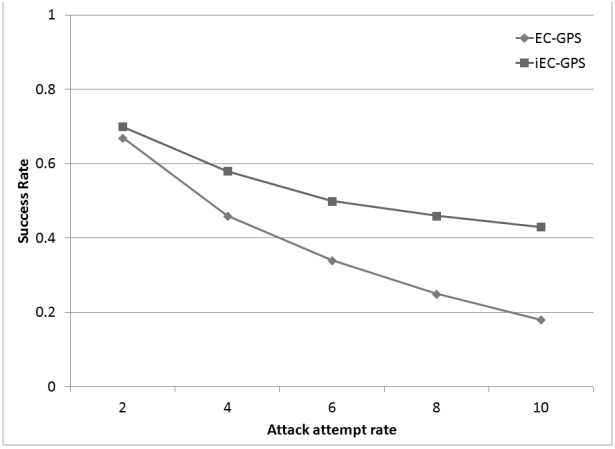

Figure 4. Success rate in EC-GPS and iEC-GPS schemes for varying attack attempt rate

Fig. 4 depicts the success rate of the authentication requests in the existing EC-GPS scheme and proposed iEC-GPS scheme while varying the attack attempt rate. It can be seen that in the existing EC-GPS scheme, success rate drastically reduced while in the proposed iEC-GPS scheme, success rate decreases soothingly. This is due to the fact that in the EC-GPS scheme, the stored coupons may get quickly exhausted for the higher attack attempt rate.

VI. CONCLUSIONS

In this paper, we have proposed a robust RFID authentication scheme for the supply-chain management system, which includes improved EC-GPS. Since the proposed scheme can resist several active attacks including DoS attacks, it is especially appropriate for the RFID deployment in open network environments.

We have provided security analysis, security proofs as well as conducted performance evaluation of the proposed scheme. It can be seen that the proposed scheme are secure and robust in terms of various security attributes, especially in terms of DoS attacks, it is superior to the existing EC-GPS scheme.

ACKNOWLEDGMENT

This work was supported by the Government of Ontario under the ORF-RE WISENSE project.

REFERENCES

[1] C.P Schnorr, ”Efficient Identification and Signatures for Smart Cards”, *in Proc of Advances in Cryptology -CRYPTO’ 89, LNCS volume 435*, pp. 239-252, Springer Berlin / Heidelberg , 1989.

[2] M. McLoone and M. J. B. Robshawn, “Public Key Cryptography and RFID Tags”, *in Proc. of Topics in Cryptology CT-RSA 2007, LNCS volume 4377*, pp. 372-384, Springer Berlin, 2007.

[3] M. Girault, G. Poupard and J. Stern, “Some modes of use of the GPS identification scheme”, *in Proc of the 3rd NESSIE Conference*, 2002.

[4] G. Hofferek and J. Wolkerstorfer, “Coupon Recalculation for the GPS Authentication Scheme”, *Smart Card Research and Advanced Applications, LNCS volume 5189*, pp. 162-175, Springer Berlin / Heidelberg, 2008.

[5] J. Cathalo, F. Koeune and J.J. Quisquater, “A New Type of Timing Attack: Application to GPS”, *in Proc. of Cryptographic Hardware and Embedded Systems - CHES 2003, Lecture Notes in Computer Science, Volume 2779*, pp. 291-303, 2003.

[6] G. Avoine, C. Lauradoux, and T. Martin, "When Compromised Readers Meet RFID", *in Proc. of Information Security Applications, WISA 2009 - Revised Selected Papers, Lecture Notes in Computer Science Volume 5932*, 2009.

[7] M. McLoone, and M.J.B. Robshaw, "New Architectures for Low-Cost Public Key Cryptography on RFID Tags", *in Proc. of IEEE International Symposium on Circuits and Systems ISCAS 2007*, pp. 1827 - 1830. New Orleans, LA, 27-30 May 2007.

[8] Y. Oren, and M. Feldhofer, “A Low-Resource Public-Key Identification Scheme for RFID Tags and Sensor Nodes”. *Proc. of the 2nd ACM conference on Wireless network security (WiSec’09)*, Mar. 2009.

[9] M. Girault, G. Poupard and J. Stern, "On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order", *Journal of Cryptology*, Volume 19, Number 4, 463-487.

[10] M. Girault, and D. Lefranc, "Public key authentication with one (online) single addition. *In Proc. of Cryptographic Hardware and Embedded Systems-CHES 2004 LNCS 3156*, pp. 967-984, 2004.

[11] M. Girault, L. Juniot, and M.J.B. Robshaw, “The Feasibility of On-the-Tag Public Key Cryptography”, *in Proc. of RFIDSec’07*, 2007.

[12] A. Shamir, "SQUASH - a new MAC with provable security properties for highly constrained devices such as RFID tags", *In Proc. of FSE, LNCS 5086,* Springer, pp. 144-157, 2008.