Optimized Security of Wireless Sensor Networks Based on a Modified Nk Cryptosystem

Tamer M. Barakat
Faculty of Engineering
Cairo University
Cairo, Egypt
tamer.barakat@bmw-eg.com

Amr M. Gody
Faculty of Engineering
Fayoum University
Fayoum, Egypt
amr.m.gody@gmail.com

Amin M. Nassar
Faculty of Engineering
Cairo University
Cairo, Egypt
aminassar@gawab.com

Abstract

Security in the wireless sensor networks (WSNs) is based on using public-key cryptosystems such as RSA cryptosystem to achieve the authentication between wireless sensor nodes and their base station. This cryptosystem has two important problems; (i) the decryption process is slow (ii) it is insecure due to some known attacks such as common modulus attack and low exponent attack.

In this paper we modify the encryption algorithm of the NK cryptosystem to avoid the problems of the RSA cryptosystem. We prove that standard attacks that applied on the RSA cryptosystem are not applicable on the NK cryptosystem after our modification.

Keywords: *Wireless Sensor Networks; RSA cryptosystem; Modified NK cryptosystem; Low exponent attack; Common modulus attack.*

1. Introduction

Wireless sensor networks are expected to be used in a wide range of applications, from monitoring wildlife and collecting microclimate data [1] to a number of military applications like target tracking [2] and detection of biological or chemical weapons. Security in the WSNs is based on using public key cryptosystem to provide privacy, data integrity, and authentication during handshaking process between wireless sensor nodes and their base station. Handshake protocol messages are encrypted using public-key cryptosystem such that RSA cryptosystem.

This cryptosystem has two problems, (i) the decryption process is slow (ii) it is insecure due to the low exponent attack and common modulus attack. Tsuyshi Takagi [3] presented a new public-key cryptosystem with fast decryption named NK cryptosystem which is constructed over $Z/\ n^k Z$, where n is the modulus and k is a positive integer. To implement the Nk cryptosystems, we used only ordinary and elementary mathematical techniques such as computation of greatest common divisors, so that it is easy to implement. Moreover, the decryption time of the first block is dominant, because after the first block we only calculate the modular multiplication of the encryption exponent and an extended Euclidean algorithm to decrypt blocks after the first one. Therefore the Nk cryptosystem is faster in the decryption process compared with the previously reported RSA-type cryptosystems [4]. If a message is several times longer than a public-key n, we can encrypt this message fast without additionally using a symmetry-key cryptosystem. This cryptosystem solves the slowness of decryption process, but it still suffers from the mentioned attacks.

This paper presents a modification of the encryption algorithm for the NK cryptosystem based on the NK to optimize security for the Wins. Therefore, the public encryption key becomes a composite number and has the relation $\bar{e} = ea$, for an integer $a \geq 1$. We prove that standard attacks such as the common modulus attack and the low exponent attack are not applicable on the NK cryptosystem after our modification.

The remainder of this paper is organized as follows: section (2) focuses on the algorithm of the modified NK cryptosystem. Proof of correctness for our construction is presented in section (3). Section (4) emphasizes on the effectiveness of low exponent attack and common modulus attack. Final section contains general conclusions.

Notation: Z is an integer ring. Z_n is a residue ring $Z/\ n^k Z$ and its complete residue class is $\{0,1,2,...,n-1\}$. Z_n^* is a reduced residue group modulo n. $LCM(m_1, m_2)$ is the Least Common Multiple of m_1 and m_2. $GCD(m_1, m_2)$ is the Greatest Common Divisor of m_1 and m_2.

2. Modification of the Nk Cryptosystem

In this section, we describe the algorithm of the modified NK cryptosystem.

2.1 The modified algorithm

1. Generation of the keys:

- Generate two random primes p, q and let $n = pq$.
- Compute $L = LCM(p-1, q-1)$ and find e, d which satisfies $ed \equiv 1 \pmod{L}$ and $GCD(e, p) = 1$, where e is the prime public encryption key before our modification and d is the corresponding secret decryption key.

- Let $\bar{e}$ be the modified public encryption key which is a composite number, where $\bar{e} = ea$, for an integer $a \geq 1$. Then $\bar{e}$, n are public keys and d, p and q are the secret keys.

2. Encryption: Let $M \in Z_n^x$ be the plaintext, we encrypt this plaintext by the following equation:

$$C \equiv \left(M_0 + nM_1 + .. + n^{k-1} M^{k-1}\right)^{ea} \left(mod\ n^k\right) \quad (1)$$

3. Decryption: First, we decrypt the first block M_0 by the secret key d;

$$M_0 = C^d \quad (mod\ n) \quad (2)$$

This is the same decryption process as in the original RSA. For the remaining blocks $M_1, M_2, ..., M_{k-1}$, we can decrypt by solving the linear equation modulo n.

2.2 Details of decryption

Assume that, we have already decrypted M_0 by the decryption method of the original RSA cryptosystem, and we write down the process to find $M_1, M_2, ..., M_{k-1}$ as follows.

Consider that the encryption function (1) is the polynomial of the variables $X_0, X_1, ..., X_{k-1}$ such that:

$$E(X_0, X_1, ..., X_{k-1}) = (X_0 + nX_1 + n^2 X_2 + ... + n^k X_{k-1})^{ea}$$

Expand the polynomial E (X_0, X.., X_{k-1}) by the polynomial theorem:

$$\sum_{\substack{0 \leq S_0, S_1, \cdots S_{K-1} \leq ey \\ S_0 + S_1 + \cdots + S_{K-1} = ey}} \frac{ea!}{S_0! S_1! \cdots S_{k-1}!} X_0^{S_0} (nX_1)^{S_1} \cdots (n^{k-1} X_{k-1})^{S_{K-1}} \quad (3)$$

And let:

$$\Gamma_i := \left\{ (S_0, S_1, ..., S_i) \middle| \begin{array}{l} S_1 + 2S_2 + ... + iS_i = i, \\ S_0 + S_1 + ... + S_i = ea, 0 \leq S_0, S_1, ..., S_i \leq ea \end{array} \right\}$$

where $(0 \leq i \leq k-1)$ and $a \geq 1$.

Let $D_i(X_0, X_1, ..., X_i)$ be the coefficient of n^i $(0 \leq i \leq k-1)$, we can find $D_i(X_0, X_1, ..., X_i)$ by calculating:

$$D_i(X_0, X_1, ..., X_i) =$$

$$\sum_{(S_0, S_1, \cdots, S_i) \in \Gamma_i} \frac{ea!}{S_0! S_1! \cdots S_i!} X_0^{S_0} X_1^{S_1} \cdots X_i^{S_i} \quad (4)$$

Here, we write them down with small i as follows:

$$D_0(X_0) = X_0^{ea} = M_0^{ea}$$

$$D_1(X_0, X_1) = eaM_0^{ey-1} M_1,$$

$$D_2(X_0, X_1, X_2) = eac_2 M_0^{ea-2} M_1^2 + eaM_0^{ea-1} M_2,$$

$$\vdots$$

$$D_{k-1}(X_0, X_1, ..., X_{k-1}) = \{ polynomial\ of\ M_0, M_1, ..., M_{k-1} \}$$

Where c_2, c_3, c_4…. are constants.

Note that: the only term that includes X_i in D_i is $eaX_0^{ea-1} X_i$.

We define:

$$D_i'(X_0, X_1, ..., X_{i-1}) = D_i(X_0, X_1, .., X_i) - eaX_0^{ea-1} X_i \quad (5)$$

Therefore, the terms $D_0, D_1, ..., D_{i-1}, D_i'$ are the polynomial of $X_0, X_1, ..., X_{i-1}$.

From this relation, we can decrypt $M_1, M_2, ..., M_{k-1}$.

Indeed, $M_1, M_2, ..., M_{k-1}$ are calculated as follows:

by setting $i = 1$, the relations

$D_1'(X_0) = 0$ and $D_0(X_0) = X_0^{ea}$.

So, the solution of the linear equation:

$eM_0^{ea-1} x \equiv B_1 \ (mod\ n)$, where $B_1 \equiv C - (D_0 M_0)\ (mod\ n^2)$,

is M_1, then we can decrypt $M_2, M_3, ..., M_{k-1}$ by solving the general linear equation:

$$eaM_0^{ea-1} x \equiv B_i \ (mod\ n), \quad (6)$$

$$B_i \equiv C - \sum_{j=0}^{i-1} D_j(M_0, M_1, ..., M_j) - D_i'(M_0, M_1, ..., M_{i-1}) \ (mod\ n^{i+1})$$

Inductively, we can decrypt all plaintexts $M_1, M_2, ..., M_{k-1}$.

3. Proof of Correctness for Our Construction

In this section, we prove the correctness for our construction which discuss how can successfully recovered the original message M after encrypt it using our modified algorithm.

3.1 Proof of correctness

From the construction of NK cryptosystem we can see that:

$$M = (M_0 + nM_1 + n^2 M_2 ..... + n^{k-1} M_{k-1}) \ (mod\ n^k)$$

Then, the value of M is correct if and only if the values of $M_0, M_1, ..., M_{k-1}$ are correct values. Therefore, we consider another assumption:

$$M = (M_0' + nM_1' + .n^2 M_2' ... + n^{k-1} M_{k-1}') \quad (mod\ n^k) \quad (7)$$

Hence, to achieve the main purpose it must be used our analysis to prove that,

$M_0' = M_0,\ M_1' = M_1, ..., M_{k-1}' = M_{k-1}$.

- ***Proof that*** $M_0' = M_0$

From equation (7) let $k = 1$ and $i = 0$. Then,

$$M = M_0' \quad (mod\ n)$$

The general linear equation that find $M_1, M_2, ..., M_{k-1}$ is given by:

$$eaM_0^{ea-1} x \equiv B_i \ (mod\ n),$$

$$B_i \equiv C - \sum_{j=0}^{i-1} D_j(M_0, M_1, ..., M_j) - D_i'(M_0, M_1, ..., M_{i-1}) \ (mod\ n^{i+1})$$

$$B_0 = C - [D_0(M_0) - eaM_0^{ea-1} M_0] = C - M_0^{ea} + eaM_0^{ea}$$

$$C = M_0^{ea}, then\ B_0 = eaM_0^{ea}$$

$$M_0' = x = \frac{B_0}{eaM_0^{ea-1}} = \frac{eaM_0^{ea} M_0}{eaM_0^{ea}} = M_0$$

Hence, the value of M_0 is correct.

- ***Proof that*** $M_1' = M_1$

Then, $k = 2$, $i = 1$ and $j = 0$.

From equation (7) $M = (M_0' + nM_1')$ $(mod\ n^2)$

The linear equation that find M_1 is

$$eaM_0^{ea-1}\, x \equiv B_1 (\bmod n),$$

$$where \quad B_1 \equiv C - D_0(M_0) - D_1'(M_0, M_1) \pmod{n^2}$$

Then, $x = M_1' = \dfrac{B_1}{eM_0^{e-1}}$

Now, we can compute each value of B_1 as follows:

The value of D_1' can be calculated by using equation (5) as follows:

$$D_1'(X_0) = D_1(X_0, X_1) - eaX_0^{ea-1} X_1$$

$$D_1'(M_0) = eaM_0^{ea-1} M_1 - eaM_0^{ea-1} M_1$$

$$then, D_1'(M_0, M_1) = 0.$$

The encryption function of M is given by the following equation:

$$C \equiv \left(M_0 + nM_1 + n^2 M_2 + ... + n^{k-1} M^{k-1}\right)^{ea} \quad \left(mod\ n^k\right)$$

In this case:

$$C \equiv (M_0' + nM_1')^{ea} \quad (mod\ n^2)$$

From the polynomial theorem we can get:

$$\sum_{(S_0, S_1, \cdots, S_i) \in \Gamma_i} \frac{ea!}{S_0! S_1! \cdots S_i!} X_0^{S_0} (nX_1^{S_1}) \cdots (n^i X_i^{S_i})$$

Where $\Gamma_i := \left\{ (S_0, S_1, ..., S_i) \middle| \begin{matrix} S_1 + 2S_2 + ... + iS_i = i, \\ S_0 + S_1 + ... + S_i = ea, 0 \le S_0, S_1, ..., S_i \le ea \end{matrix} \right\}$

Then, $C = M_0^{ea} + eanM_0^{ea-1} M_1$

Hence, $B_1 = eaM_0^{ea-1} M_1 + M_0^{ea} - M_0^{ea} = eaM_0^{ea-1} M_1$

Then, $M_1' = \dfrac{B_1}{eaM_0^{ea-1}} = \dfrac{eaM_0^{ea-1} M_1}{eaM_0^{ea-1}}$

Then, $M_1' = M_1$

Hence, the value of M_1 is correct.

By the same manner, we can prove that the values of $M_2, ..., M_{k-1}$ are the correct values. So that our construction is correct to recover the original message after encrypt it using the proposed cryptosystem.

4. The Modified Nk Cryptosystem Immunity to the Existing Attacks

In this section, we explain the effectiveness of low exponent attack and common modulus attack against the NK cryptosystem after modification.

4.1 Low exponent attack

A low public exponent is desirable to reduce encryption time. However, there is a powerful attack on low public exponent for NK cryptosystem as well as RSA cryptosystem based on a theorem due to Coppersmith [5]. Hastad reported an attack, named low exponent attack based on Coppersmith's theorem, which detects a low public exponent e. This attack is effective for $H \ge e$, where H is a number of parities that receive the same message M at the same time with common public exponent e; on the other hand the public key for the modified NK cryptosystem has the relation: $\bar{e} = ea$, for an integer $a \ge 1$. Therefore, if the attacker can achieve Coppersmith's constraint such that $H \ge ea$, then, our modified cryptosystem will be broken.

Here, we discuss Hastad's attack. For simplicity, suppose that the same message M has to be sent to three different users and all corresponding public exponents are equal to 3. Therefore, the modified public key becomes $\bar{e} = ea$ = 3*2, where a =2.

Let the original message $M = 4$. Then, we calculate the modulus n for each message as follows:

For message #1:

$p_1 = 3,\ q_1 = 5, n = 15\ and\ k = 2 \Rightarrow n_1^k = 2025.$

For message #2:

$p_2 = 3,\ q_2 = 7, n_2 = 21\ and\ k = 2 \Rightarrow n_2^k = 441.$

For message #3:

$p_3 = 5,\ q_3 = 7, n_3 = 35\ and\ k = 2 \Rightarrow n_3^k = 1225.$ Then, the corresponding ciphertexts are:

$$C_1 = (4)^6 \mod 2025 = 46,$$

$$C_2 = (4)^6 \mod 441 = 127, \quad and$$

$$C_3 = (4)^6 \mod 1225 = 421.$$

Applying the Chinese Remainder Theorem (CRT) to C_1, C_2, and C_3 as follows:

$$M^6 = C_1 + C_2 + C_3 \pmod{N}$$

$$M = 2 \pmod{496125}$$

Therefore, the attacker gets the value of message equal 2 whereas the original message is equal 4. Then, the attacker gets a hard problem, he always gets the wrong value of the message M. this means that he did not know if the value of message M is true or false. This problem takes place because Coppersmith's constraint is not satisfied. To successfully mount this attack he must get at least six messages to satisfy Coppersmith's constraint, but this way will increase the effort of the attacker to recover the correct value of the original message. Then, when using the modified NK cryptosystem with small public exponent, the attacker will meet a hard problem when attempt to break this system using low exponent attack. The following tables summarize the numbers of messages required to mount a successful Hastad's attack.

Table 1. The number of messages required to mount a successful Hastad's attack for NK cryptosystem before our modification. Note that: the system is not defined for even values of e.

e	3	5	7	9	11	13
# of messages	4	6	8	10	12	14

Table 2. The number of messages required to mount a successful Hastad's attack for NK cryptosystem after our modification. Note that: (*) means that the attack is not applicable which means that the attacker meets a hard computation to get the correct value of the original message.

e	$\bar{e}$ (a =2)	# of messages
3	6	7
5	10	11
31	62	*

From Table 1 we observe that, at $e = 3$, the attacker just needs four messages to successfully break the NK cryptosystem, whereas at $\bar{e} = 6$ in Table 2 the attacker will need at least seven messages to break that cryptosystem.

4.2 Common modulus attack

Simmon pointed out in [6] that the use of a common RSA modulus is dangerous, indeed, if a message M is sent to two users that have comprised public encryption keys, then the message can be recovered. On the other hand, the NK cryptosystem presented by Tsuyoshi Takagi also suffer from this attack because the public encryption key still prime number. Here, we discuss the effectiveness of the common modulus attack on the security of the modified NK cryptosystem. Suppose that we need to send a message M to two users that have the ciphertexts given by:

$C_1 \equiv M^{\bar{e}_1} \pmod n$ and $C_1 \equiv M^{\bar{e}_2} \pmod n$, where $\bar{e}_1, \bar{e}_2$ are the public encryption keys for common modulus (n = pq) for the modified NK cryptosystem.

The attacker attempts to break this system using one of the following methods:

Method #1:

From our modification, we can see that $gcd(\bar{e}_1, \bar{e}_2) \neq 1$ because these values become a composite numbers. So, when the attacker attempt to use extended Euclidean algorithm to find u, v such that $u\bar{e}_1 + v\bar{e}_2 = 1$, where u *and* v are non-negative integers, he fail to satisfy this equation because $\bar{e}_1, \bar{e}_2$ are composite numbers, i.e. $u\bar{e}_1 + v\bar{e}_2 \neq 1$.

Therefore, he cannot use the following relation to recover the original message:

$$M \neq M^{u\bar{e}_1 + v\bar{e}_2} \not\equiv C_1^u C_2^v \pmod n$$

Method #2:

The attacker succeeds to factorize the composite public key $\bar{e}_1, \bar{e}_2$ to $\bar{e}_1 = e_1 * a$ *and* $\bar{e}_2 = e_2 * a$ respectively.

Then, he begins his attempt to recover the original message as follows:

Let $u\bar{e}_1 + v\bar{e}_2 = 1$

Then, $u e_1 a + v e_2 a = 1$

$(ua)e_1 + (va)e_2 = 1$

$u' e_1 + v' e_2 = 1 \implies$ This relation can be obtained from extended Euclidean algorithm.

Therefore, $M = M^{u' e_1 + v' e_2} \implies M = [M^{e_1}]^{u'} * [M^{e_1}]^{v'}$ (8)

But, $M^{e_1} \neq C_1$ as well as $M^{e_2} \neq C_2$.

So, the attacker cannot use equation (8) to recover the original message.

Hence, the common modulus attack seems infeasible for the modified PKQ cryptosystem.

5. Conclusions

This paper addressed one of the important topics in mobile networks, which is security in the WSNs. When we need to achieve the authentication between wireless sensor nodes and their base station in WSNs, we must use strong public-key cryptosystem rather than RSA cryptosystem which is currently use for authentication process in WSNs because the RSA cryptosystem suffers from some known attacks such as low exponent attack and common modulus attack. Therefore, we presented a modified of the encryption algorithm for the NK cryptosystem. According to our modification, we conclude that the modified NK cryptosystem is secure against the common modulus attack because the public encryption key became a composite number. On the other hand, we showed that it is possible to use the NK cryptosystem with a composite small encryption key $\bar{e}$ provided Coppersmith's condition $H < \bar{e}$, where H is the number of parties that receive the same message at the same time. This condition is used to defend against the low exponent attack. Therefore, the Low exponent Attack seems infeasible. From this paper we choose the modulus n to be for example 1024-bit for the 341-bit primes p and q, in order to make both the elliptic curve method and the number field sieve infeasible. So, this modulus is secure against the fast factoring algorithms.

Finally to optimize the security of WSNs we may use the modified NK cryptosystem to achieve secure authentication between wireless sensor nodes and their base station.

6. Acknowledgements

I would like to thank prof. Amin Nassar and Dr. Amr Gody for their continuous encouragement supervision, guidance, suggestions and assistance through all the stages of this paper.

7. References

[1] A. Polastre, J. Szewczyk, R. Culler, " D. Anderson. Wireless Sensor Networks for habitat monitoring, " First ACM Workshop on Wireless Sensor Networks and Applications, Atlanta, GA, USA. 2002.

[2] Burne R., " Self-organizing co-operative sensor network for remote surveillance: improved target traking results, " In proceedings of the SPIE. Volume 4232. Boston, SPIE, SPIE-Int. Soc. Opt. Eng, USA 2001, 313-321.

[3] T. Takagi, "New public-key cryptosystem with fast decryption," Advances in Cryptology (PhD Thesis) - LNCS 1294, Germany, 2001.

[4] N. Demytko, "A new elliptic curve based analogue of RSA," Advances in Cryptology {EUROCRYPT '93, LNCS 765, (1994), pp.40-49.

[5] D.Coppersmith, "Small solutions to polynomials equations and low exponent RSA vulnerabilities," 1996

[6] G. L. Simmons, "A 'weak' privacy protocol using the RSA crypto algorithm," Cryptologia 7 1993, pp. 180-182.

Biographies

Amin M. Nassar: Received BSc. from Cairo University, in 1965, in electronics and communication engineering. He is earned PhD in electronics and communication engineering in 1973 from Germany. He is professor in Cairo University in electronics and communication department.

Amr M. Gody: Joined Cairo University, faculty of Engineering in 1986. He is earned BSc. in Electronics and communication engineering in 1991 with distinction with an honor degree and top 5% in the class. Amr is working in the area of signal processing staring from 1993. The field of specialization is speech signal

processing. He is earned the M.Sc degree in Electronics and communication engineering in 1995 from Cairo University, faculty of Engineering. He is joined the PhD program in Cairo university in 1996. He is earned the PhD in 1999 in the field of speech signal processing.
Amr is Assistant professor in Fayoum University, Electrical engineering department and he is a member in IEEE.

Tamer M. Barakat: Joined Helwan University, faculty of Engineering in 1995. He is received BSc. in communication engineering in 2000. He is earned the M.Sc degree in communication engineering from Helwan University in 2004. The filed of specialization is computer security. He is joined the PhD program in Cairo University in 2005.