Providing Hop-by-Hop Authentication and Source Privacy in Wireless Sensor Networks

Yun Li[†], Jian Li[†], Jian Ren[†] and Jie Wu[‡]

[†]Department of ECE, Michigan State University
[‡]Department of CIS, Temple University

March 26, 2012

Outline

1. Introduction
   - Message Authentication
   - Existing Algorithms
2. Proposed Scheme
   - Main Idea
   - Terminology
   - Proposed Source Anonymous Message Authentication (SAMA) Scheme
   - AS Selection and Source Privacy
3. Performance Analysis
   - Theoretical Performance Analysis
   - Experimental Performance Analysis

Message Authentication

System Model and Assumptions

- A wireless sensor network consists of a large number of sensor nodes.
- After deployment, the sensor nodes may be captured and compromised by attackers.
- A security server (SS) is responsible for generating, storage and distribution of the security parameters.
- SS will never be compromised.

Message Authentication

- Plays a key role in thwarting unauthorized and corrupted packets from being circulated in networks.
- Saves precious sensor energy.

Existing Algorithms

Polynomial Based Message Authentication

- The idea is similar to threshold secret sharing.
- Advantages: The scheme offers information theoretic security.
- Disadvantages: When the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system is completely broken.

Recent Anonymous Communication Protocol

- The idea is based on ring signatures.
- Advantages: This protocol enables the message sender to generate a source anonymous message signature with content authenticity assurance.
- Disadvantages: The original scheme has very limited flexibility and very high complexity.

Main Idea

Main Idea

- Apply the optimal modified ElGamal signature (MES) scheme on elliptic curves.
- Propose an unconditionally secure and efficient source anonymous message authentication (SAMA) schemes.

Terminology

SAMA

A SAMA consists of the following two algorithms:

- Generate $(m, Q_1, Q_2, \ldots, Q_n)$: Given a message m and the public keys $Q_1, Q_2, \ldots, Q_n$ of the AS (ambiguity set) $\mathcal{S} = \{A_1, A_2, \ldots, A_n\}$, the actual message sender A_t,$1 \leq t \leq n$, produces an anonymous message $\mathcal{S}(m)$ using its own private key d_t.
- Verify $\mathcal{S}(m)$: Given a message m and an anonymous message $\mathcal{S}(m)$, which includes the public keys of all members in the AS, a verifier can determine whether $\mathcal{S}(m)$ is generated by a member in the AS.

Terminology

Modified ElGamal Signature Scheme (MES)

- Key generation algorithm: Let p be a large prime and g be a generator of Z_p^*. Both p and g are made public. For a random private key $x \in Z_p$, the public key y is computed from $y = g^x \mod p$.
- Signature algorithm: One chooses a random $k \in Z_{p-1}$, then computes the exponentiation $r = g^k \mod p$ and solves s from $s = rxh(m, r) + k \mod (p-1)$, where h is a one-way hash function. The signature of message m is defined as the pair (r, s).
- Verification algorithm: The verifier checks whether the signature equation $g^s = ry^{rh(m,r)} \mod p$: If the equality holds true, then the verifier Accepts the signature, and Rejects otherwise.

Proposed MES Scheme on Elliptic Curves

Proposed MES Scheme on Elliptic Curves

- Let $p > 3$ be an odd prime. An elliptic curve E is defined as $E : y^2 = x^3 + ax + b \bmod p$, where $a, b \in \mathcal{F}_p$, and $4a^3 + 27b^2 \not\equiv 0 \bmod p$.
- The set $E(\mathcal{F}_p)$ consists of all points $(x, y) \in \mathcal{F}_p$ on the curve, together with a special point $\mathcal{O}$, called the point at infinity.
- $G = (x_G, y_G)$ is a base point on $E(\mathcal{F}_p)$ whose order is a very large value N.
- User A selects a random integer $d_A \in [1, N-1]$ as his private key. Then, he can compute his public key Q_A from $Q_A = d_A \times G$.

Proposed MES Scheme on Elliptic Curves

Signature Generation Algorithm

For Alice to sign a message m, she follows these steps:

1) Select a random integer k_A, $1 \leq k_A \leq N-1$.
2) Calculate $r = x_A \bmod N$, where $(x_A, y_A) = k_A G$. If $r = 0$, go back to step 1.
3) Calculate $h_A \xleftarrow{l} h(m, r)$, where h is a cryptographic hash function, such as SHA-1, and $\xleftarrow{l}$ denotes the l leftmost bits of the hash.
4) Calculate $s = r d_A h_A + k_A \bmod N$. If $s = 0$, go back to step 2.
5) The signature is the pair (r, s).

Proposed MES Scheme on Elliptic Curves

Signature Verification Algorithm

Bob can follow these steps to verify the signature:

1) Verify that r and s are integers in $[1, N-1]$. If not, the signature is invalid.
2) Calculate $h_A \xleftarrow{l} h(m, r)$, where h is the same function used in the signature generation.
3) Calculate $(x_1, x_2) = sG - rh_A Q_A \bmod N$.
4) The signature is valid if $r = x_1 \bmod N$, invalid otherwise.

Proposed SAMA on Elliptic Curves

Proposed SAMA on Elliptic Curves

- Alice wishes to transmit a message m anonymously from her network node to any other nodes.
- The AS includes n members, $A_1, A_2, \ldots, A_n$, e.g., $\mathcal{S} = \{A_1, A_2, \ldots, A_n\}$, where the actual message sender Alice is A_t, for some value $t, 1 \leq t \leq n$.
- In this paper, we will not distinguish between the node A_i and its public key Q_i. Therefore, we also have $\mathcal{S} = \{Q_1, Q_2, \ldots, Q_n\}$.

Proposed SAMA on Elliptic Curves

Authentication Generation Algorithm

The SAMA of the message m is defined as: $\mathcal{S}(m) = (m, \mathcal{S}, r_1, y_1; \ldots, r_n, y_n, s)$ after the following steps:

1) Select a random and pairwise different k_i for each $1 \le i \le n-1, i \ne t$ and compute r_i from $(r_i, y_i) = k_i G$.
2) Choose a random $k_i \in \mathbb{Z}_p$ and compute r_t from $(r_t, y_t) = k_t G - \sum_{i \ne t} r_i h_i Q_i$ such that $r_t \ne 0$ and $r_t \ne r_i$ for any $i \ne t$, where $h_i \xleftarrow{l} h(m, r_i)$.
3) Compute $s = k_t + \sum_{i \ne t} k_i + r_t d_t h_t \bmod N$.

Proposed SAMA on Elliptic Curves

Authentication Verification Algorithm

Bob can follow these steps to verify the signature:

1) Verify that $r_i, y_i, i = 1, \cdots, n$ and s are integers in $[1, N-1]$. If not, the signature is invalid.
2) Calculate $h_i \xleftarrow{l} h(m, r_i)$, where h is the same function used in the signature generation.
3) Calculate $(x_0, y_0) = sG - \sum_{i=1}^{n} r_i h_i Q_i$
4) The signature is valid if the first coordinate of $\sum_i (r_i, y_i)$ equals x_0, invalid otherwise.

Proposed SAMA on Elliptic Curves

Remark 1

It is apparent that when $n = 1$, SAMA becomes a simple signature algorithm.

Theorem 1

The proposed source anonymous message authentication scheme (SAMA) can provide unconditional message sender anonymity.

Theorem 2

The proposed SAMA is secure against adaptive chosen-message attacks in the random oracle model.

AS Selection and Source Privacy

AS Selection and Source Privacy

- Before a message is transmitted, the message source node selects an AS from the public key list in the SS as its choice.
- The adversary is unable to distinguish whether the previous node is the actual source node or simply a forwarder node.
- Therefore, the selection of the AS should create sufficient diversity.

Performance Analysis

Performance Analysis

- We compare our proposed scheme with the bivariate polynomial-based symmetric-key scheme in both theoretical aspect and experimental aspect.
- A fair comparison of our proposed scheme and the bivariate polynomial scheme should be performed with $n = 1$.

Theoretical Performance Analysis

Bivariate Polynomial Scheme

The secret bivariate polynomial is defined as

$$f(x,y) = \sum_{i=0}^{d_x} \sum_{j=0}^{dy} A_{i,j} x^i y^j$$

- Considering the message length and the computational complexity, d_x and d_y should be as short as possible.
- The intruders can recover the polynomial $f(x,y)$ via Lagrange interpolation if one of the two things below happens:
  - Either more than $d_y + 1$ messages transmitted from the base station are received and recorded by the intruders
  - Or more than $d_x + 1$ sensor nodes have been compromised.
- This property requires that both d_x and d_y be very large.

Theoretical Performance Analysis

Summary of SAMA's Advantages

- For $n = 1$, our scheme can provide at least the same security as the bivariate polynomial-based scheme.
  - Our scheme can provide the authentication without the threshold constrain.
  - Our scheme is proved to be secure in the random oracle model.
- For $n > 1$, we can provide extra source privacy benefits.
  - Our design enables the SAMA to be verified through a single equation without individually verifying the signatures.
  - The secure is unconditional. Every node in the AS has the equal probability of sending the messages.

Experimental Performance Analysis

Parameter Setup

- The bivariate polynomial-based scheme is a symmetric-key based implementation, while our scheme is based on ECC.
- If we choose the key size to be l for the symmetric-key cryptosystem, then the key size for our proposed ECC will be $2l$.
- We choose five security levels, which are indicated by the symmetric-key sizes l: 24bit, 32bit, 40bit, 64bit, and 80bit.
- The comparable key sizes of our scheme are 48bit, 64bit, 80bit, 128bit, and 160bit, respectively.

Experimental Performance Analysis

Computational Overhead

We first performed simulation to measure the process time in the 16-bit, 4 MHz TelosB mote.

TABLE I
PROCESS TIME (S) FOR THE TWO SCHEMES (16-BIT, 4 MHZ TELOSB MOTE)

	Polynomial based approach						Proposed approach							
	$d_x, d_y = 80$		$d_x, d_y = 100$		$d_x, d_y = 150$		$n = 1$		$n = 10$		$n = 15$		$n = 20$	
	Gen	Verify	Gen	Verify	Gen	Verify	Gen	Verify	Gen	Verify	Gen	Verify	Gen	Verify
l = 24	9.31	0.25	14.45	0.31	31.95	0.46	0.24	0.53	4.24	2.39	6.16	3.51	8.38	4.44
l = 32	12.95	0.33	20.05	0.41	44.60	0.62	0.34	0.80	5.99	3.32	8.92	5.05	12.19	6.42
l = 40	13.32	0.35	20.57	0.44	45.73	0.65	0.46	1.05	8.03	4.44	11.94	6.71	16.18	8.50
l = 64	21.75	0.57	33.64	0.71	74.85	1.06	1.18	1.77	20.53	11.03	30.12	16.41	41.44	21.10
l = 80	26.40	0.70	41.03	0.88	90.86	1.30	1.46	2.22	25.58	13.90	37.66	20.96	50.96	26.18

Experimental Performance Analysis

Computational Overhead

Below is the comparison of memory consumption in the 16-bit, 4 MHz TelosB mote.

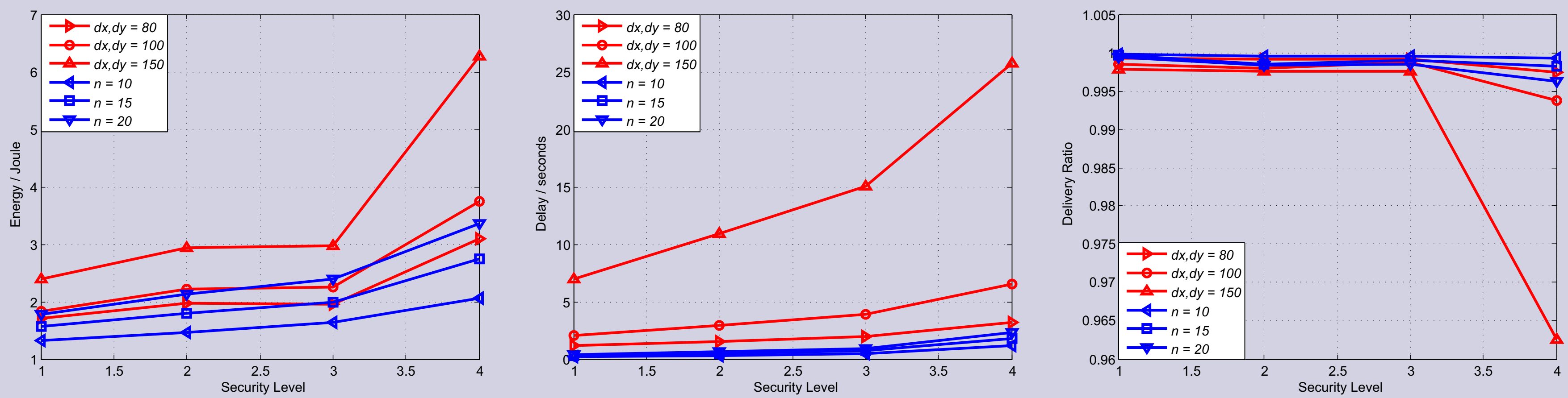
TABLE II
MEMORY (KB) AND TIME (S) CONSUMPTION FOR THE TWO SCHEMES (TELOSB) (F STANDS FOR FLASH MEMORY).

	Polynomial based approach									Proposed approach											
	$d_x, d_y = 80$			$d_x, d_y = 100$			$d_x, d_y = 150$			$n = 1$			$n = 10$			$n = 15$			$n = 20$		
	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F
$l = 24$	21	3	26	21	4	40	26	4	90	21	1	0	21	2	0	21	2	0	21	2	0
$l = 32$	21	4	39	21	5	60	26	6	135	21	2	0	21	2	0	21	2	0	21	2	0
$l = 40$	21	4	39	21	5	60	26	6	135	21	2	0	21	2	0	21	2	0	21	3	0
$l = 64$	21	6	64	21	7	100	26	9	225	21	2	0	22	3	0	22	3	0	22	3	0
$l = 80$	21	7	77	21	8	120	26	10	270	20	2	0	21	3	0	21	3	0	21	4	0

Experimental Performance Analysis

Performance Comparison

The simulation results for energy consumption, transmission delay and delivery ratio were carried out in ns-2.



(a) (b) (c)

Fig. 1. Performance comparison of our proposed scheme and bivariate polynomial-based scheme: (a) energy consumption, (b) message delay, (c) delivery ratio

Conclusion

In the paper, we

- develop a source anonymous message authentication (SAMA) scheme on elliptic curves that can provide unconditional source anonymity.
- offer an efficient hop-by-hop message authentication mechanism without the threshold limitation.
- devise network implementation criteria on source node privacy protection in WSNs.
- provide extensive simulation results under ns-2 and TelosB on multiple security levels.
- demonstrate that our scheme not only has efficiency in authentication but also can provide extra source privacy.

Thank you! Questions?