Computers and Electrical Engineering 39 (2013) 1880–1893

Contents lists available at SciVerse ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Performance analysis of multivariate cryptosystem schemes for wireless sensor network ☆

Pradheepkumar Singaravelu *, Shekhar Verma

Department of Information Technology, Indian Institute of Information Technology, Allahabad, India

ARTICLE INFO

Article history:
Available online 11 August 2012

ABSTRACT

In a wireless sensor networks (WSN), large numbers of tiny sensor devices observe their environment and communicate the observation to a sink. Security is vital to avoid false reporting, safety of sensors and sensed objects. In particular, message authentication is crucial to prevent false response that may be evoked by a message. This necessitates a strong cryptographic mechanism to ensure safety. However, existing resource intensive cryptographic mechanisms are can affect the performance and lifetime of a WSN adversely. To address this problem of security in resource limited WSN, multivariate cryptosystem schemes are proposed and evaluated in this paper. The viability of different multivariate cryptosystems have been analyzed on the anvil of computation and memory requirements. Simulation results show that multivariate cryptosystem require small computation time and low memory that make them viable for security provisioning in a WSN. Results also show that the throughput of the network is large with low average delay even with large number of sensor nodes.

1. Introduction

A WSN consists of tiny low cost devices equipped with sensors and transreceivers that sense data and then cooperate among themselves to forward data to the sink [1]. Both sensor nodes and sensed data are vulnerable and security concerns are a serious impediment to widespread adoption of sensor networks. WSN pose unique security implementation challenges viz., low communication bandwidth, wireless broadcast channel, limited memory, limited power and low processing capability. The broadcast nature [2,3] of the channel makes data susceptible to intrusion, interception, injection and modification. Data confidentiality, forward secrecy, privacy and integrity are, therefore, required to protect the nodes and information in transit. The resource constraints [4,5] make security provisioning a challenging task. The existing security primitives [6,7] require large size keys for encryption/decryption/signature validation to satisfy the sensor security needs. Existing cryptographic schemes such as Diffie–Hellman, Rivest, Shamir and Adleman (RSA) and Elliptic curve cryptosystem (ECC) require large computational power and memory which a tiny sensor node does not possess.

Symmetric key cryptosystems require storage of pairwise keys in all nodes in the network in the pre-deployment stage or using an efficient key distribution scheme, however, both are resource intensive. Moreover, compromise of a few nodes leads to compromises of the entire network. For example, RSA [8] requires complicated computation and long period of key-setup time since it performs a univariate monomial operation over a very large ring. Moreover, most of these techniques drain the battery. To overcome these problems two paths exist; one, multivariate polynomials over small finite fields and second, use of monomials as the public key and hiding data in the exponent that leads to the discrete logarithm over complicated groups.

☆ Reviews processed and recommended for publication to Editor-in-Chief by Guest Editor Prof. Mehdi Shadaram.
* Corresponding author.
E-mail addresses: spradheepkumar@iiita.ac.in (P. Singaravelu), sverma@iiita.ac.in (S. Verma).

0045-7906/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.compeleceng.2012.07.010

Compared to the RSA and ECC schemes, systems based on the discrete logarithm over elliptic curves are capable of maintaining the same security level with shorter key sizes. The low complexity and shorter length of the keys make ECC attractive for implementation on sensor motes. However, the shortest signature that can be produced using an elliptic curve digital signature algorithm (ECDSA) is too long for most sensor nodes [8]. Multivariate cryptosystems over small fields are very fast as compared to RSA and ECC. Their security is based on the difficulty of solving multivariate polynomial equations. Multivariate cryptography [9] comprises all the cryptographic schemes that use multivariate polynomials over finite fields. They are faster since arithmetic operations on large units (RSA or ECC) are replaced by operations on many small units. The primary idea is to choose a multivariate system F of quadratic polynomials which can be easily inverted. After that two affine linear invertible maps S and T are chosen to hide the structure of the central map. The public key of the cryptosystem is the composed map $P = S \circ F \circ T$ which is difficult to invert. The private key consists of S, F and T and therefore allows P by inversion. There are several ways to build the central map F. Matsumoto and Imai (MI scheme), is one of the big field schemes [10] that is used for encryption and signature. Both secret and public transformations in C^* scheme [11] can be done in much less than $O(N^3)$ complexity. Internal perturbation of MI scheme (PMI) is an extension and generalization of MI scheme. In the construction of PMI scheme [12], a small dimensional subspace is used to produce the perturbation. HFE [13,14] uses polynomial equation over finite fields. A signature scheme based on HFE called Quartz has been proposed in [15]. On the other hand, oil and vinegar (OV) scheme [16] and Rainbow multivariate signature scheme are single field family schemes. OV scheme uses quadratic polynomials in which oil variables can only appear linearly. With the set of OV polynomials, solutions for the oil variables produce a signature. OV scheme [16] is very efficient and provides fast signature generation and verification. Rainbow multivariate signature scheme [17,18] is a variant of OV scheme. It has a set of embedded layer which uses several instances of the OV construction layers. This allows Rainbow multivariate signature scheme to improve upon the efficiency of the original OV scheme. The Rainbow multivariate signature scheme is believed to be secure against attacks. Medium field [19] schemes have been proposed as third family of multivariate cryptosystems which contain schemes like ℓ-iC scheme [20]. The objective of the present work is to determine the viability of these cryptosystem schemes for WSN and compare their performance against the ECC based scheme with respect to computational needs and memory required for intermediate and final output. The rest of the paper is organized as follows. Section 2 gives the problem definition. Section 3 describes the existing cryptosystem for WSN with details of ECC based scheme. Multivariate cryptographic schemes are detailed in Section 4. Section 5 contains the performance analysis of the simulation results. The conclusions are given in Section 6.

2. Problem definition

The tasks of sensing, computation and communication by sensor nodes consume energy. The energy consumption pattern determines the operational lifetime of a typical node. Battery depletion increases with the amount of computation and communication. Since, communication is energy intensive, the message size and the number of attempts for successful transmission largely determines the battery life. Thus, a cryptographic technique for WSN must have small memory footprints and lesser number of attempts for successful transmission to ensure communication efficiency. The number of operations must also be low so that the technique is computationally energy efficient. However, reduction in computation and size must not compromise security. Traditional public key cryptosystems are energy intensive requiring significant computational power and storage. To address this problem, multivariate cryptosystem can be employed for WSN. There were different types of multivariate cryptosystems with slightly varying resource requirements. The feasibility of a particular scheme for WSN depends on its computation requirements, memory required for storage of intermediate results and size of the final output. Various types of sensor motes are available and have different characteristics features like operating system, programming and processors. Moreover, implementations of the cryptographic schemes are time consuming and may not convey adequate information about the efficiency of the schemes. Hence, benchmarking of different types of multivariate cryptosystem against a common scheme is required. Since ECC scheme is currently the most promising candidate for security provisioning, benchmarking multivariate cryptosystems used to be benchmarked against ECC scheme is necessary to determine their viability in the WSN environment.

3. Existing WSN cryptosystem schemes

Private and public key cryptography have been proposed to satisfy the different security requirements of sensor networks. Their effectiveness has been evaluated with respect to their security strength and their efficiency in the resource constrained WSN environment. In [21], the energy consumption was measured with respect to the computational overhead for different platforms like Amega103, PXA250 and UltraSparc2 for different encryption algorithms like RC4, IDEA, RC5 and hash algorithms like MD5 and SHA1 for predicting node performance. The impact of security overhead on memory usage and energy consumption on Mica2 motes with a CC1000 radio was evaluated for security algorithms like TEA, Skipjack and RC5 with TinySec in [21]. Their results show Skipjack consumes more energy than RC5 and TEA. The effect of block ciphers on memory usage using the standard modes of operation is evaluated in [22]. However, the energy consumption has not been studied. The extra energy spent when hash functions and symmetric-key algorithms are used is measured in Mica2 motes [23,24]. Multi-user authentication schemes with security strength, storage efficiency and communication efficiency has been studied in [25]. This scheme is based on the efficient integration of Bloom filter, the partial message recovery signature