ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Secure Data Aggregation in Wireless Sensor Network Using Source Privacy Based Elliptic Curve Cryptography

Karuna Sagar, Bharath. M. B

M. Tech Student, Dept. of Computer Science & Engineering, Rajeev Institute of Technology, Hassan, India

Assistant Professor, Dept. of Information Science & Engineering, Rajeev Institute of Technology, Hassan, India

ABSTRACT: Wireless sensor network is a collection of large number of low cost resource constraint sensor nodes that communicates using wireless medium. Sensor nodes are resource constrained in memory, sensing, communication capability, and battery power. Data communication between nodes consumes a large portion of the total energy consumption of the WSNs. One of the solutions to reduce number of bits transmitted during communication is data aggregation. As wireless sensor networks are usually deployed in remote and hostile environments to transmit sensitive information, sensor nodes are prone to attacks. Collusion attack also main constraint which has to be considered while transmitting a secure data. Thus, security is an important criterion to be considered in WSNs. Many secure data aggregation protocols have been proposed in wireless sensor networks. In this project, we are using key distribution technique to aggregate and to maintain the secrecy of data. We propose a Source privacy based based on elliptic curve cryptography (SP-ECC). While enabling intermediate nodes authentication, our proposed scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem.

KEYWORDS: Elliptic Curve Cryptography, Source Privacy, Message authentication.

I. INTRODUCTION

A sensor (also called detector) is a converter that measures a physical quantity and converts it into a signal. The collection of individual sensor nodes can be connected into a wireless sensor network and the principal tasks are nodecomputation, storage, communication, and sensing. The components which are required to perform this task can be roughly categorized into three categories Passive, Omni-directional sensors. These sensors can measure a physical quantity at the point of the sensor node without actually manipulating the Environment by active probing. – In this sense, they are passive [2] [3]. There is no notion of "direction" involved in these measurements. Examples for such sensors include thermometer, light sensors, vibration, Microphones, humidity, mechanical stress or tension in materials, chemical sensors sensitive for given substances, smoke detectors, air pressure, and so on. – Passive, narrow-beam [2] [3] sensors these sensors are passive as well, but have a well-defined notion of direction of measurement. A typical example is a camera, which can "take measurements in a given direction, but has to be rotated if need be. – Active sensors this last group of sensors actively probes the environment, for example, a sonar or radar sensor or some types of seismic sensors.

Remote Sensor Networks (WSN) are developing as both an imperative new level in the IT biological community and a rich area of dynamic examination including equipment and framework outline, organizing, dispersed calculations, programming models, information administration, security and social components. The fundamental thought of sensor system is to scatter minor detecting gadgets; which are equipped for detecting a few changes of episodes/parameters and speaking with different gadgets, over a particular geographic territory for a few particular purposes like target following, reconnaissance, ecological checking and so on. Toady's sensors can screen temperature, weight, dampness, soil cosmetics, vehicular development, clamor levels, lighting conditions, the vicinity or nonattendance of specific sorts of articles or substances, mechanical anxiety levels on joined articles, what's more, different properties. If there should be an occurrence of remote sensor system, the correspondence among the sensors is finished utilizing remote handsets. Essentially the significant test for utilizing any effective security plan in remote sensor systems is made by the extent of

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

sensors, thus the handling force, memory and sort of errands anticipated from the sensors. Security is an extensively utilized term incorporating the attributes of validation, respectability, security, nonrepudiation, and against playback. The more the reliance on the data gave by the systems has been expanded, the more the danger of secure transmission of data over the systems has expanded. For the protected transmission of different sorts of data over systems, a few cryptographic.

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions. The development of such networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control. Data collected by sensors is transmitted to a special node equipped with higher energy and processing capabilities called "Base Station" (BS) or "sink". The BS collects filters and aggregates data sent by sensors in order to extract useful information.

Analysis on wireless sensor networks a bit reason for diminish the lifetime of sensor networks are power Consumption, frequent radial of data to nodes, load traffic, overhead of message passing, energy hole between the nodes and sink nodes. Because LEACH depends on only a probabilistic model, some cluster heads may be very close each other and can be located in the edge of WSNs. These inefficient cluster heads could not maximize the energy efficiency.

The main objective of our algorithm is to prolong the lifetime of the WSN by evenly distributing the workload. To achieve this goal, we have mostly focused on selecting proper CHs from existent sensor nodes. LEACH-ERE selects the CHs considering expected residual energy of the sensor nodes.

In our proposed system Fuzzy based LEACH-ERE along with Handoff Mechanism is used for Enhancing the network lifetime. LEACH-ERE is used in cluster formation based on energy of nodes remained. Handoff Mechanism used for efficient cluster head selection and data transmission that helps in maintaining lifetime for loner period.

II. RELATED WORK

Ismail Mansour et. al. focused on key management issues in multi-hop wireless sensor networks. These networks are easy to attack due to the open nature of the wireless medium. Intruders could try to penetrate the network, capture nodes or take control over particular nodes. In this context, it is important to revoke and renew keys that might be learned by malicious nodes. We propose several secure protocols for key revocation and key renewal based on symmetric encryption and elliptic curve cryptography. All protocols are secure, but have different security levels. Each proposed protocol is formally proven and analyzed using Scyther, an automatic verification tool for cryptographic protocols. For efficiency comparison sake, we implemented all protocols on real testbeds using TelosB motes and discussed their performances.

Sweta Nigam et. al. authentication scheme based on elliptic curve cryptography (ECC) is used to allow any node to transmit and authenticate an unlimited number of messages without suffering the threshold problem and provides message source privacy.

III. PROBLEM STATEMENT

Due to limited computational power and energy resources, aggregation of data from multiple sensor nodes done at the aggregating node is usually accomplished by simple methods such as averaging. However such aggregation is known to be highly vulnerable to node compromising attacks. Since WSN are usually unattended and without tamper resistant hardware, they are highly susceptible to such attacks. Thus, ascertaining trustworthiness of data and reputation of sensor nodes is crucial for WSN.

IV. PROPOSED SYSTEM

In this section, we describe the aggregation model and the attack model. The aggregation model defines how aggregation works, and the attack model defines what kinds of attacks our secure data aggregation scheme should protect against.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

A. Aggregation Model

We consider large scale WSNs with densely deployed sensors. In WSNs, there are three types of nodes: base station (BS), aggregator, and leaf node. In this paper, we consider the aggregation tree roots at the BS like general data aggregation protocol. Sensor nodes have overlapping sensing regions due to the dense deployment, and the same event is often detected by multiple sensors. Hence, data aggregation is proposed to reduce data transmission. The non-leaf nodes, except the BS, may also serve as aggregators. They are responsible for combining answers from their child nodes and forwarding intermediate aggregation results to their parents. Without loss of generality, we focus on additive aggregation, which can serve as the base of other statistical operations.

B. Attack Model

First, we categorize the abilities of the adversary as follows:
(1) An adversary can eavesdrop on transmission data in a WSN.
(2) An adversary can send the forged data to leaf nodes, aggregators, or BS.
(3) An adversary can compromise secrets in sensors or aggregators.

Then, we define five attacks to qualify the security strength of the secure data aggregation schemes, based on adversary's abilities and purposes.

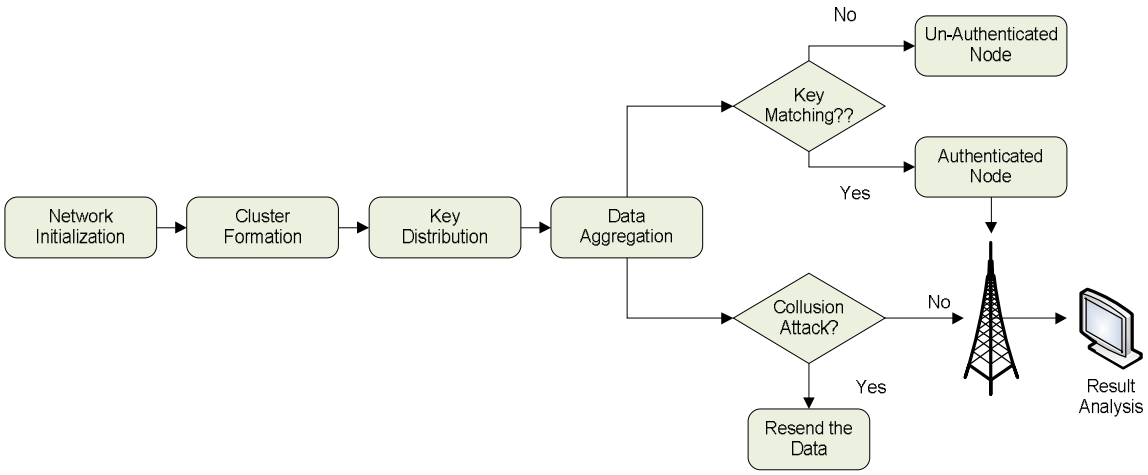

Figure 1: Architecture of Proposed System

SP-ECC Message Authentication: In this section, we propose an unconditionally secure and efficient SP-ECC. The main idea is that for each message m to be released, the message sender, or the sending node, generates a source anonymous message authenticator for the message m. The generation is based on the MES scheme on elliptic curves. For a ring signature, each ring member is required to compute a forgery signature for all other members in the AS. In our scheme, the entire SP Massage authentication generation requires only three steps, which link all non-senders and the message sender to the SP alike. In addition, our design enables the SP-ECC message authentication to be verified through a single equation without individually verifying the signatures.

Let p > 3 be an odd prime. An elliptic curve E is defined by an equation of the form:

$$E: y^2 = x^3 + ax + b \bmod p, \qquad (1)$$

Where $a, b \in F_p$, and $4a^3 + 27b^2 \neq 0 \bmod p$. The set $E(F_p)$ consists of all points $(x, y) \in F_p$ on the curve, together with a special point O, called the point of infinity.

Let $G = (x_G, y_G)$ be a base point on $E(F_p)$ whose order is a very large value N. User A selects a random integer $d_A \in [1, N-1]$ as his private key. Them, he can complete his public key Q_A from $Q_A = d_A \times G$.

Signature generation algorithm as follows.

Step1: select a random integer k_A, $1 \leq k_A \leq N-1$.

Step2: Calculate $r = x_A \bmod N$, where $(x_A, y_A) = k_A G$. If r=0, go back to step 1.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Step3: Calculate . If r=0, go back to step 1.

Step3: Calculate $h_A \overset{l}{\leftarrow} h(m, r)$, where h is a cryptographic has function, such as SHA-1, and $\overset{l}{\leftarrow}$ denotes the l leftmost bits of the hash.

Step4: Estimate $s = rd_A h_A + k_A \bmod N$. If s=0, go back to step 2.

Step5: the signature is the pair (r, s).

Signature Verification algorithm is as follows:

Lets say for Sender authenticate the receiver signature, the receiver must have the public key Q_A, then the algorithm steps follows as shown below.

Step1: Checks that $Q_A \neq 0$, otherwise invalid

Step2: Checks that Q_A lies on the curve.

Step3: Checks that $nQ_A = 0$

After, sender follows 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. Results and Discussions:

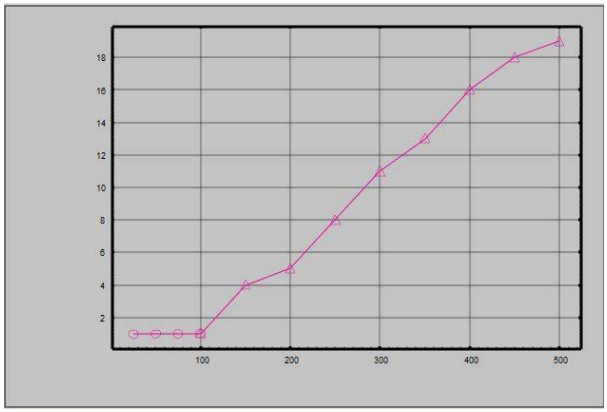

Figure 2: Energy Consumption as the number of nodes increases. Where x axis represents energy in joules and y axis represents the number of nodes.

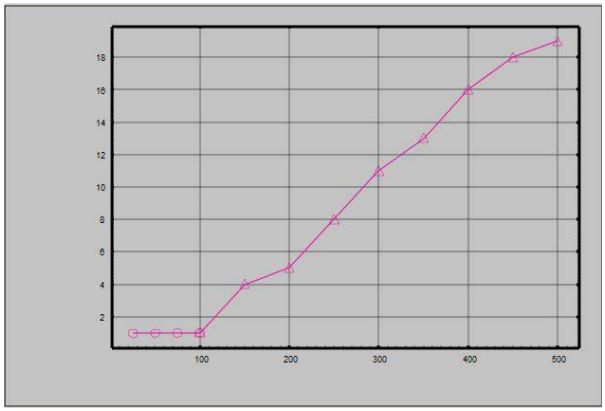

Figure 3: Packet Delivery ratio

V. CONCLUSION

Privacy, Source privacy based ECC can be applied to any message to provide message content authenticity. To provide hop-by-hop message authentication without the weakness of the builtin threshold of the polynomial-based

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

scheme, we then proposed a hop-by-hop message authentication scheme based on the SP-ECC. When applied to WSNs with fixed sink nodes, we also discussed possible techniques for compromised node identification. We compared our proposed scheme with the bivariate polynomial-based scheme through simulations using ns-2. Both theoretical and simulation results show that, in comparable scenarios, our proposed scheme is more efficient than the bivariate polynomial-based scheme in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption.

REFERENCES

[1] F. Ye, H. Lou, S. Lu, and L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM, Mar. 2004.
[2] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-By-Hop Authentication Scheme for Filtering False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004.
[3] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking Cryptographic Schemes Based on 'Perturbation Polynomials'," 2009.
[4] Lejla Batina, Nele Mentens, Kazuo Sakiyama, Bart Preneel, and Ingrid Verbauwhede, "Low-Cost Elliptic Curve Cryptography for Wireless Sensor Networks", Springer, pp. 6–17, 2006.
[5] Sweta Nigam and K.N. Hande, "Survey on "Security Architecture Based on ECC (Elliptic Curve Cryptography) in Network", International Journal of Computer Science and Mobile Applications, Volume 3, Issue 1, 2015.
[6] Mehala.G and Mariselvi.J, "Source Anonymous Message Authentication in Security Networks", International Journal of Computer Trends and Technology, volume 17, Issue 3, 2014.
[7] Chinnaswamy C.N and Natesha B V, "Message Authentication between the Nodes using modified El-Gamal Signature on Elliptic Curve", International Journal for Advance Research in Engineering and Technology, Volume 2, Issue 5, 2014.
[8] Naipunya H C, Nalina G R, Gururaj H L and Ramesh B, "Secured Source Anonymous Message Authentication Using Wireless Sensor Network", Journal of Computer Engineering, Volume 17, Issue 3, 2015.