International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in; editorijoer@gmail.com

Vol.4., Issue.6., 2016
Nov-Dec.

RESEARCH ARTICLE

ISSN: 2321-7758

# FALSE DATA FILTERING SCHEME USING ECDSA IN WIRELESS SENSOR NETWORK

**P.RAJESHWARI[1], S.REKHA[2]**

[1,2]Assistant Professor, Computer Science and Engineering
Gojan School of Business and Technology, 80 Feet Road, Edapalayam, Red hills,
Chennai
p.rajeshwari@gojaneducation.com[1];srekha@gojaneducation.com[2]


**ABSTRACT**
A wireless sensor network is a group of specialized transducers for monitoring and recording conditions at diverse locations. A sensor network consists of multiple detection stations called sensor nodes .Every sensor node is equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena. The microcomputer processes and stores the sensor output. The transceiver receives commands from a central computer and transmits data to that computer. These sensor nodes are deployed in the unattended environment .So there is a chances of intruder can easily capture and inject a false data in the sensor node. The false reports make the server misjudge and not respond the real situation immediately. Moreover, false decision depletes the energy of sensor nodes and the server and it also creates threat to the lifetime of the sensor nodes. To deal with this issue, the paper proposed elliptical curve cryptography message authentication scheme for safely transfer the data and to filter out the false injected data.

**Keywords:** Sensor network, Message authentication, ECC, Key distribution.



## I. INTRODUCTION

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks .WSAN are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. In such environment sensor nodes are subjected to various types of attacks such as eavesdropping, masquerade, false data injection, selective forwarding. Sensor nodes sense the events and generate event report for the sensed information and the event report has to be send to the base station .When event report is forwarded; a

compromised node can forge the report. False data contain false information from compromised nodes. The false data injection attack depletes the energy of the sensor nodes. One solution to reduce the impact of false data injection into the network through a compromised node is to filter the false data by elliptical curve cryptography message authentication method for safely transfer the report to the base station.

## II. LITERATURE REVIEW

**TICK SCHEME :** The communication cost is the most dominant factor in a sensor's energy consumption. Thus, in TICK, instead of explicitly "chatty" schemes. Sensor node use their local time value as a one-time dynamic key to encrypt each message. The receiving node use their local time to intelligently decode the timing key of the source node. As time progresses, the following transmissions use different time values. TICK is also an effective dynamic en-route filtering mechanism. Where the malicious is filtered out from the network. To the best of our knowledge earlier dynamic en-route filtering schemes for WSNs have not taken this approach. Both analytical and simulation results verified the feasibility of the TICK scheme and presented that TICK was more energy-efficient than other comparable schemes.

**AERF SCHEME:** In our scheme, each node uses its own auth-keys to authenticate their reports and a legitimate report should be endorsed by nodes. The auth-key of each node form a hash chain and are updated in each round. The cluster-head disseminates the first auth-key of every node to forwarding nodes and then sends the reports followed by disclosed auth-key. The forwarding nodes verify the authenticity of the disclosed keys by hashing the disseminated keys on forwarding the reports. The process is repeated by each forwarding node at every hop. A major challenge for a wireless sensor networks lies in the energy constraints at each node, which poses fundamental limit on the network life time

**BECAN SCHEME:** In this paper, a different BECAN scheme is proposed for filtering the injected false data based on Bloom filter. This proposed approach is efficient and can be used for making theoretical analysis on the relevant works. It is observed from the experiments that the BECAN scheme can achieve better En-routing filtering probability and improved reliability with multi-reports. The performance of the packet delivery ratio end-to-end latency and throughput of the proposed system achieved in the stimulation experiments. The result show that the proposed system impresses performance on energy consumption, security of data and also communication cost. This BECAN also be applied on other distributed authentication scenario since it prevents and authorized access through injecting false data attack from mobile compromised sensor nodes through routing protocols

**TOWARDS A TRUST COMPUTING ARCHITECTURE FOR RPL IN CYBER PHYSICAL SYSTEM:** The RPL standard allows secure modes, but keying details are left out. Our approach is to use a TPM, which provides accurate and tamper-proof data in insecure environments, while ensuring integrity and authenticity of received messages. We designed a trust establishment and key exchange mechanism around the implied trust a TPM offers, to provide keys for secure RPL modes. Unlike other approaches, this ensures that nodes only provide keys to and use those supplied by trustworthy nodes. Using a TPM on RCDs reduces the processing load on the main processor. With our approach, dissemination of misleading routing information, which affects the availability of the whole network, can be effectively prevented by using a TPM.

**SECURE CONTROL: TOWARDS SURVIVABLE CYBER-PHYSICAL SYSTEMS**: Cyber-Physical Systems (CPS) integrates computing and communication capabilities with monitoring and control of entities in the physical world. These systems are usually composed by a set of networked agents, including: sensors, actuators, control processing units, and communication devices. While some forms of CPS are already in use, the widespread growth of wireless embedded sensors and actuators is creating several new applications –in areas such as medical devices, autonomous vehicles, and smart structures– and increasing the role of existing ones –such as Supervisory Control and Data Acquisition (SCADA) systems.

**A NOVEL EN-ROUTE FILTERING SCHEME AGAINST FALSE DATA INJECTION ATTACKS IN CYBER-PHYSICAL NETWORKED SYSTEMS**

PCREF adopts polynomials instead of MACs (Message Authentication Codes) for endorsing measurement reports to achieve the resilience to attacks. Each node stores two types of polynomials: authentication polynomial and check polynomial, derived from the primitive polynomial, and used for endorsing and verifying the measurement reports. this scheme and its extensions all have the weakness of a built in threshold determined by the degree of the polynomial when the number of messages transmitted is larger than this threshold cannot be transmitted

**III. PRELIMINARY**

**A. The Basis of En-route Filtering**

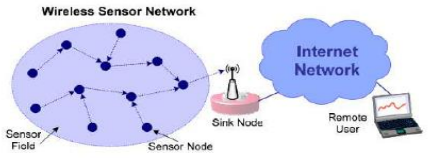
Generally speaking, en-route filtering is a scheme by which intermediate nodes check the authenticity of messages and filter them when those messages travel the network. En-route filtering can reduce the number of hops that the false messages travel over the network. En-route Filtering is an energy efficient scheme as the false messages are filtered at intermediate nodes before posing the impact on remaining nodes in the path. The false message (or report) forged by compromised sensor nodes can consume lots of network and computation resources and shorten the lifetime of sensor net-works and CPNS. Therefore, false reports should be filtered at forwarding nodes as quickly as possible. Most of the existing en-route filtering schemes are based on *T* authentication, i.e., a legitimate measurement report must carry at least *T* valid message authentication codes (MACs) generated by different valid sensor nodes in CPNS, where *T* is the threshold and pre-defined before CPNS is deployed. When a report is transmitted from a sensor node to the controller, each forwarding node checks whether the forwarding reports actually carry *T* valid MACs. If not, the report is considered as a false one forged by the adversary and then dropped. Otherwise, the report is forwarded to the next forwarding nodes along the route. This process ensures that false reports can be filtered along the route as quickly as possible before arriving at the controller. In this paper, our proposed ECDSA is based on this basic idea to conduct en-route filtering against false reports

B. Network and Threat Models

There are two types of nodes in the system: sensing nodes and forwarding nodes, shown as green nodes and red node. These two types of nodes are denoted as sensor nodes in the paper. Note that, two nodes is connected with bi-directional link means that these two nodes are within each other's wireless communication range and can communicate with each other directly. The sensing nodes can not only sense and form the measurement reports of the monitored components, but also forward the measurement reports of other nodes. The forwarding nodes can only forward the measurement reports to the controller. We assume that each cluster has a unique cluster ID and each node has a unique node ID. Sensor nodes that measure or forward measurement reports have a limited computation and communication capability and limited energy resources. Sensor nodes lack tamper-resistance hardware and can be compromised by the adversary. An example of system model, where nodes *v*1, *v*2, *v* 3, and *v*4 obtain the measurement reports of monitored component *j* and send them to the controller through *v*4. Similarly, *u*4 sends the measurement report of monitored component *i* to the controller through multiple forwarding nodes. We can see that *v*1 can serve as a forwarding node to transmit the measurement reports of monitored component *i*.

We assume that the adversary can compromise sensor nodes, including both the sensing nodes and forwarding nodes. Once a node is compromised, the secret information stored in the node becomes visible to the adversary. The adversary can inject false measurement reports to the controller through the compromised nodes. This causes the controller to estimate wrong system states and send wrong control commands to the actuators, posing dangerous threat to the system. The false reports also consume network and computation resources and shorten the lifetime of CPNS. We assume that the controller is well protected and the adversary can only obtain

the authentication information through compromising sensor nodes.




Architecture of WSN

**IV. EXISTING SYSTEM**

In existing en-route filtering schemes uses a polynomial based Message Authentication. In this scheme two types of nodes are considered, they are sensing node and forwarding node. The sensing node can not only sense, but also forward the measurement reports along the route, whereas the forwarding node is used to forward the received measurement reports to the controller. Each node stores two types of polynomials: authentication polynomial and check polynomial, which are derived by different primitive polynomials. Each sensing node stores the authentication polynomial of local cluster and the check polynomial of other clusters with a pre-defined probability. Each forwarding node stores the check polynomial of each cluster with the same probability. It assigns the authentication polynomial and check polynomial for each node based on the cluster-based polynomial assignment, i.e., nodes in different clusters are assigned different primitive polynomials and generate different *authentication polynomial* and *check polynomial*. this scheme and its extensions all have the weakness of a built in threshold determined by the degree of the polynomial when the number of messages transmitted is larger than this threshold cannot be transmitted .the adversary can fully recover the polynomial and the system is broken completely.

**V. PROPOSED SYSTEM**

***A. Basic Idea***

In our proposed system, we propose a elliptic curve cryptography (ECC), where all participating devices have a pair of keys called "private key" and "public key." The private key is used by the originator to sign a message, and the recipient uses the originator's public key to verify the authenticity of the signature. If a message is modified on its way to the recipient, the signature verification fails because the original signature is not valid for the modified message. The Digital Signature Standard (DSS), issued by the National Institute of Standards and Technology (NIST), specifies suitable elliptic curves, the computation of key pairs, and digital signatures.

*Step 1:* **Network Topology**

Each node sends "hello" message to other nodes which allows detecting it. Once a node detects "hello" message from another node (neighbor), it maintains a contact record to store information about the neighbor. Using multicast socket, all nodes are used to detect the neighbor nodes.

*Step 2:* **Cluster Updating and Key Distribution:**

In a cluster, each monitored component is monitored by *n* sensing nodes and it can communicate with each other nodes. We assign the cluster name to each cluster and each sensing node stores its cluster name. Each cluster can communicate with the help of forwarding sensors. Each sensing nodes can sense the data and forward the data to the forwarding sensors. Then the measured data can be forwarded to the controller with the help of forwarding nodes..

*Step 3:* **Secure Data Forwarding**:

En-route Filtering is an energy efficient scheme as the false messages are filtered at intermediate nodes before posing the impact on remaining nodes in the network. The false message (or report) forged by compromised sensor nodes can consume lots of network and computation resources and shorten the lifetime of sensor networks. Therefore, false reports should be filtered at forwarding nodes as quickly as possible by using the secret key.

**VI. ECDSA AUTHENTICATION SYSTEM**

An ellipsis is a special case of the general second-degree equation $ax^2 + bxy + cy^2 + dx + ey + f = 0$. Depending on the values of the parameters a to f, the resulting graph could be a circle, hyperbola, or parabola. Elliptic curve cryptography uses third-degree equations. The DSS defines two kinds of elliptic curves for use with ECC: pseudo-random curves, whose coefficients are generated from the output of a seeded cryptographic hash function; and special curves, whose coefficients and

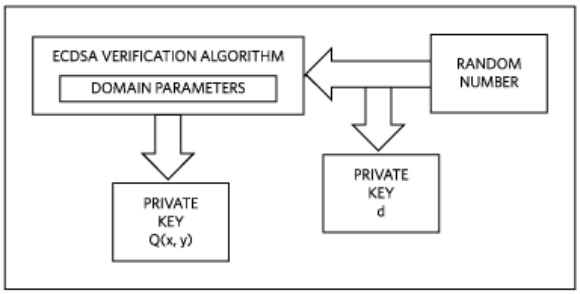
underlying field have been selected to optimize the efficiency of the elliptic curve operations. Pseudo-random curves can be defined over prime fields GF(p) as well as binary fields GF(2m). A prime field is the field GF(p), which contains a prime number p of elements. The elements of this field are the integers modulo p; the field arithmetic is implemented in terms of the arithmetic of integers modulo p. The applicable elliptic curve has the form $y^2 = x^3 + ax + b$. A binary field is the field GF(2m), which contains 2m elements for some m (called the degree of the field). The elements of this field are the bit strings of length m; the field arithmetic is implemented in terms of operations on the bits. The applicable elliptic curve has the form $y^2 + xy = x^3 + ax^2 + b$. Although there is a virtually unlimited number of possible curves that meet the equation, only a small number of curves is relevant for ECC. These curves are referenced as NIST Recommended Elliptic Curves in FIPS publication 186. Each curve is defined by its name and domain parameters set, which consists of the Prime Modulus p, the Prime Order n, the Coefficient a, the Coefficient b, and the x and y coordinates of the Base Point G(x,y) on the curve

**A. Mathematical Background**

Elliptic curve cryptography involves scalars and points. Typically, scalars are represented with lower-case letters, while points are represented as upper-case letters, as in Table 1. Three numerical operations are defined for scalars: addition (+), multiplication (*) and inversion ($^{-1}$). There are two numerical operations for points: addition (+) and multiplication (×). Although the symbol "+" is used for scalars and points, a point addition follows different rules than the scalar addition. These operations apply to curves over prime fields, as well as curves over binary fields. Algebraic formulae to perform these computations. Computations needed for ECDSA authentication are the generation of a key pair (private key, public key), the computation of a signature, and the verification of a signature. The corresponding equations are found in public literature.

**B. Key Pair Generation**

Before an ECDSA authenticator can function, it needs to know its private key. The public key is derived from the private key and the domain parameters. The key pair must reside in the authenticator's memory. As the name implies, the private key is not accessible from the outside world. The public key, in contrast, must be openly read accessible



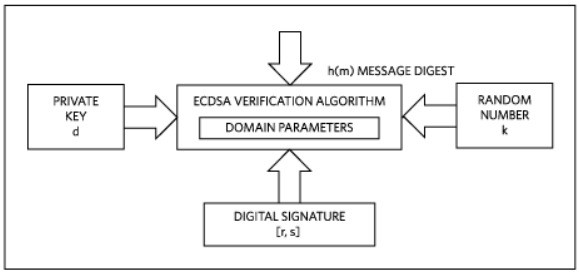

*Key pair generation process.*

A random number generator is started and, when its operation is completed, delivers the numeric value that becomes the private key d (a scalar). Next, the public key Q(x,y) is computed according to Equation 1 through point multiplication:

$$Q(x, y) = d \times G(x, y) \qquad \text{(Eq. 1)}$$

**C. Signature Computation**

A digital signature allows the recipient of a message to verify the message's authenticity using the authenticator's public key. First, the variable-length message is converted to a fixed-length message digest h(m) using a secure hash algorithm. A secure hash has the following distinctive properties: 1) irreversibility—it is computationally infeasible to determine the message from its digest; 2) collision resistance—it is impractical to find more than one message that produces a given digest; and 3) high avalanche effect—any change in the message produces a significant change in the digest. After the message digest is computed, a random number generator is activated to provide a value k for the elliptic curve computations. **Figure 3** illustrates the process.




*Signature computation process.*

from the random number k and the base point G(x,y):

$(x1, y1) = k \times G(x, y) \bmod p$ (Eq. 2)
$r = x1 \bmod n$

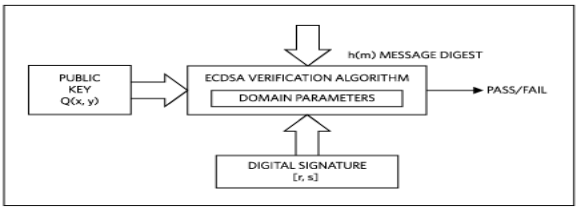
To be valid, r must be different from zero. In the rare case when r is 0, a new random number, k, must be generated and r needs to be computed again .After r is successfully computed, s is computed according to Equation 3 using scalar operations. Inputs are the message digest h(m); the private key d; r; and the random number k:

$s = (k^{-1} (h(m) + d * r) \bmod n$ (Eq. 3)

To be valid, s must be different from zero. If s is 0, a new random number k must be generated and both r and s need to be computed again.

**D. Signature Verification**

The signature verification is the counterpart of the signature computation. Its purpose is to verify the message's authenticity using the authenticator's public key. Using the same secure hash algorithm as in the signature step, the message digest signed by the authenticator is computed which, together with the public key Q(x,y) and the digital signature components r and s, leads to the result. **Figure 4** illustrates the process.




*Signature verification process.*

Equation 4 shows the individual steps of the verification process. Inputs are the message digest h(m), the public key Q(x,y), the signature components r and s, and the base point G(x,y):

$w = s\text{-}1 \bmod n$
$u1 = (h(m) * w) \bmod n$
$u2 = (r * w) \bmod n$ (Eq. 4)
$(x2, y2) = (u1 \times G(x, y) + u2 \times Q(x, y)) \bmod n$

The verification is successful ("passes"), if x2 is equal to r, thus confirming that the signature was indeed computed using the private key.

**VII CONCLUSION**

In this paper, we proposed aN elliptic curve cryptography has a low complexity mainly because the group's members have the same key pairs, but also because the authentication is made through zero knowledge. Using elliptic curve cryptography provides a methodology for obtaining high-speed implementations of authentication protocols and encrypted message techniques while using fewer bits for the keys. For establishing the encryption/decryption keys we chose a method were no point on the elliptic curve is made public. Keeping the elliptic curve point private increases the security of the algorithm. This method is also easy to implement, being based on the characteristics elliptic curves and RSA encryption systems.The developed scheme achieves better filtering capacity, Energy Efficiencies and resilience to a large number of compromised nodes in comparison with the existing schemes.

**REFERENCES**

[1]. Time-Based Dynamic Keying and En-Route Filtering (TICK) for Wireless Sensor Networks proposed by A. SelcukUluagac , Raheem A. Beyah, John A. Copeland

[2]. An Active En-Route Filtering Scheme For Secured Data Dissemination in Wireless Sensor Networks proposed by N.Parashuram, Y.Sanjaysai raj, A.Sagar, B.Uma.

[3]. Lightweight and Compromise-Resilient Message Authentication in Sensor Networks proposed byWensheng Zhang and Nalin Subramanian, Guiling Wang.

[4]. Detecting False Data in Wireless Sensor Network using Efficient BecanScheme proposed by S.Sajithabanu, M.Durairaj

[5]. Towards A Trust Computing Architecture for RPL in Cyber Physical System proposed by Sebastian Seeber, AnujSehgaly, BjörnStelte, Gabi DreoRodosek, Jürgen Schönwäldery

[6]. Secure Control: Towards Survivable Cyber-Physical Systems proposed by Alvaro A. C ardenasSaurabh Amin Shankar Sastry

[7]. A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked Systems by Xinyu Yang