Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 44 (2023), No. 7, pp. 1327–1346
DOI : 10.47974/JIOS-1286

Prolong the lifetime of sensor monitoring system using schedule matrix while employing digital signatures

Pankaj Kumar *
Saurabh Kumar Sharma †
School of Computer and Systems Sciences
Jawaharlal Nehru University
New Delhi
India

Kaveri Umesh Kadam §
Department of Electronics and Communication Engineering
Jamia Millia Islamia Central University
New Delhi
India

Abstract

In this paper a linear programing approach has been implemented for finding the energy efficient path for prolonging the network lifetime of sensor monitoring systems. For a given set of sensors and spots, a sensor can only monitor a single spot at a time and a spot can be the monitoring range of k-sensors. While using digital signatures on sensor nodes, a linear programming framework is designed to determine the system's maximum life time. Digital signatures provide node authentication and non-repudiation service in wireless sensor network. Non-repudiation is supported by different types of digital signature schemes. Such schemes have large communication and /or computation cost, which is traditionally infeasible for wireless sensor network. The proposed solution addresses such issue by using a scheduling mechanism. The problem is divided into three steps: (i) using a linear programming approach, determine the system's maximum life-time and make an assignment matrix. (ii) The assignment matrix is factored into a series of scheduling matrices. (iii) On the basis of schedule matrices that indicate the group of active sensors determine the optimal path of data flow from node-i to node-j.

Subject Classification: *68M18.*

Keywords: *Digital signature, Monitoring system, Scheduling algorithm, Wireless sensor network, Scheduling matrix.*

* *E-mail:* **pankajkumar.scss.jnu@gmail.com (Corresponding Author)**
† *E-mail:* **saurabhsharma.lpu@gmail.com**
§ *E-mail:* **gf.kkadam@jmi.ac.in**

1. Introduction

A wireless sensor network (WSN) is comprised of autonomous inexpensive and energy efficient sensor nodes that collectively monitored physical or environment related activities i.e., pressure, motion, noise, temperature, pollutants or vibration at various spots. The main application of wireless sensor networks includes environmental monitoring, traffic monitoring, military sensing, building structures monitoring etc. Strengthen power budget of sensor node is the major feature of sensor networks; because the nodes in WSN are usually energized by batteries that are not rechargeable or swapped once they are set up in adverse environmental conditions. A longer life-time is required for sensor network to keep monitoring the physical or environmental conditions. Extending the life-time of WSN is a significant research theme. It is very difficult for a designer of wireless sensor network to design the most energy efficient solution because of limitation in power budget in wireless sensors. In many decision-making activities in sensor surveillance systems, sensor node authenticity and integrity of data are crucial. As a result, before transferring the data to the sink node, the sensor node must digitally sign all pertinent data. The sink node should be the only one with permission to verify digitally signed data [1].

For user authentication in cryptography, the Digital Signature Standard is employed. Therefore, it is possible to effectively encrypt messages and digital signatures using a public key issued as an encryption key by some recognized authority and a private key generated from the public key. A type of encryption known as homomorphic encryption [2] enables certain computations to be conducted on cypher text and produces an encrypted result that, when decrypted, is identical to the outcome of operations carried out on the plaintext.

There is no single digital signature scheme which is most suited for a particular design problem. Communication-computation trade-offs appear while applying digital signature on surveillance sensor nodes. Communication/computation challenges arise throughout the error control [3], modulation process [4], cryptography key exchange [5], and many other processes [6, 7].

The proposed solution uses scheduling matrix approach to find the energy efficient path by applying digital signature on sensor nodes. It consists of a group of collaborating sensor nodes that detect and track moving objects and communicate their locations to the sink node of wireless sensor network. Initially each sensor is equipped with preliminary energy,

fixed monitoring range and flexible communication range. One sensor node can monitor only one spot at one time; however, one spot can be the monitoring zone of multiple sensors. Each spot is assumed to be tracked by *k*-sensors, where $k \geq 1$. A linear topology of wireless sensor network has been used and the position of spots and sensor nodes are static.

Because sensors are redundantly deployed in monitoring systems, the proposed model schedules a subgroup of sensors to be awake at time t_1, another subgroup at time t_2, and so on to monitor the spots and determine the best path to transfer the collected data to the sink node, ensuring that each spot is monitored by k-sensors at all times. As a result, the system's lifetime can be extended.

The life-time of monitoring system can be defined as "the time interval between when at least one spot cannot be monitored by k-sensors and when data cannot be transmitted to the sink node due to sensor node energy depletion".

The layout of this article is structured as: Section 2 discussed the similar work. Section 3 elaborates the research reviews of many authentications scheme used in WSN. The proposed model, with a linear programming formulation, assignment matrix creation, schedule matrices, and the k-matching technique, are all explained in Section 4. Section 5 describes all about the experimental setup. Section 6 explains the simulation and experimental results analysis work. Section 7 concludes the solution.

2. Literature Review

Many studies have been conducted on how to extend the life time of sensor networks. The study of the upper limit of life-time of sensor networks used to gather data in diverse courses of events is explained by Bhardwaj et al. [8]. For a few cases, their simulation findings obtained upper bounds that are close to the ideal, and for the remainder, they are very close. To compute the bound of life-time, a different technique is used, which subdivides the problem into sub-problems with well-known or easily obtained bounds. In a sensor network, a monitoring service for various spot-areas is discussed by L.B. Ruiz et al. [9]. It is built on a low-energy coverage sensing mechanism that covered certain geographic areas. Its simulation results imply that in WSN, a longer life-time and reduced transmission cost can be achieved.

To maximize the life-time of a sensor network, another strategy based on switch on/off mode of sensor nodes is introduced by R.A. Brualdi and H.J. Ryser [10]. Full coverage, distributing requests, and data aggregation

are three characteristics of energy efficiency. The optimal strategy is to turn off as many sensors nodes as feasible at once without impacting their functionality.

M.L. Sichitiu [11] investigated a static permanent monitoring sensor network, which is based on a distributed scheduling mechanism and is time synchronized. The time scale difference only occurs when it's time to enable sensors during network reconfiguration and data forwarding. Its simulation results demonstrate that the network life-time can be significantly increased.

One more node scheduling model is designed [12] to turn off/ on sensor nodes without affecting its functionality. It works on its local information that is monitor by its neighbor. When a node's monitoring region is monitored by a neighbor, a node decides to turn off. This operation will continue until a node's monitoring region is smaller than the specified boundary value.

Sang and Arora [13] proposed "Spatial Signature" for crypto-free authenticated transmission in WSN. For the implementation of spatial signature, the physical features of the signal (Signal intensity factor, Link performance factor, etc.) that the sensor node generates at neighbor nodes are used. The false positive rate is shown to be less than 6% based on simulation findings. This approach could be used in a WSN for sensor node authentication where the application of digital signature is not possible.

Seys and Preneel [14] compare the consumption of energy of various digital signature algorithms on less power consumption appliances. Finally, they suggest that the Elliptic Curve Digital Signature Algorithm (ECDSA) is the best option because it is simple to use and uses just 2.5-7 times the amount of computing power as the One-Time Signature (OTS).

For the maximum life-time routing problem in WSN, Chang and Tassiulas [15] propose a linear programming approach. They discovered that if all data packets are sent along the same way, the battery power of nodes along that path depletes more quickly than on other routes.

Ergen and Varaiya [16] investigate the life-time of WSNs utilizing two linear programming modal routing techniques. One such method is to extend the life of each sensor node, while another aims to reduce the amount of energy used for data transmission. The ratio of transmitting energy and circuit energy is the deciding factor to make a routing decision.

Liu et al. [17] propose the maximum life-time scheduling strategy for sensor monitoring systems with k-sensors to monitor a single site.

Bicakci et al. [18] examine the communication/computation trade-offs for increasing the life-time of a wireless sensor network using digital signatures for node authentication. They employ a linear programming problem to recommend ideas for making optimal use of this trade-offs in order to extend the network's life.

3. Digital Signature Algorithm

Digital signature techniques that can be used in WSN include ECDSA, RSA, OTS, Lightweight digital signatures, and Identity-based signatures. When used in the WSN, they each have their own set of benefits and drawbacks. Because energy budgets are restricted, WSN designers must make every effort to find the most energy-efficient solution possible.

For sensor node authentication, Kalita and Kar [19] suggested a key management approach. In this system, an authenticated node can only identify the public key of the base station/sink node, and a single hop key confirms the public key of a newly inserted node. When delivering the public key of the base station to new sensor nodes, two-factor authentication is essential to prevent unlawful node insertion into the network. Mahmud and Aktar [20] suggested a method in which all registered nodes share a secret key. To communicate with another node, a node must first send an authentication message to that node. When a message is validated, a particular node starts communicating. For digital signatures and network verification, they used an identity-based elliptic curve cryptography approach. Ren et al. [21] suggested a bloom filter-based authentication system that stores the authenticated node identification in a bloom filter. This strategy, however, is subject to a denial-of-service (DoS) attack, as well as fabricated data and the usage of the bloom filter by the attacker. A shared secret key mechanism-based method was presented by Abror et al. [22].

The ECDH (Elliptic-Curve Diffie–Hellman) key exchange mechanism is used to produce and exchange the shared secret key. In the ECDH key exchange, the SHA-1 function is used to produce message MAC values and to ensure message integrity via authentication. A trust authority system that uses both a public and a secret key was developed by Mohator et al. [23]. The key derivation function generates node secret keys by using a base station secret key as a starting point. The node uses the secret key to generate the message's signature before sending it to another node for verification. To ensure the network's permitted access, Perring et al. [24] proposed the μTESLA system. It generates a key chain for sensor node

authentication using a one-way hash algorithm. Nodes, on the other hand, necessitate the maintenance of a long key chain. Furthermore, μTESLA is affected by severe denial-of-service assaults. The received messages must be buffered and then verified using the key broadcasted by the base station at each sensor node. To solve the difficulty of broadcast authentication in WSN, Zhou and Fang [25] proposed a novel approach named BABRA. It solves the difficulty of maintaining μTESLA's extensive key chain. It is, however, vulnerable to denial-of-service attacks. Cao et al. [26] presents an identity-based signature technique for multiuser broadcast authentication. Before broadcasting a message to the network, a node must sign it using the vBNN-IBS signature method.

The (Generate, Sign, Verify) is a digital signature system with the security parameter l and $n \in poly(l)$. The key generator function (*Generate)* accepts the security parameter 1^n as an input and returns a key pair (*pk,sk*). Where *pk* is a public key and *sk* is a private key of length *n. Sign* is a signature generation algorithm that accepts two inputs: a private key (*sk)* and a message (*m)* and return a signature (*s)* as an output (i.e $s \leftarrow Sign_{sk}(m)$). *Verify* is a signature verifier function that takes three parameters: public key (*pk)*, signature (*s)* and message (*m)* and returns *v*. (i.e $v \leftarrow Verify_{pk}(m,s)$); the signature (*s)* is considered to be valid if $v = 1$.

Along with the proposed method, this study incorporates three different digital signature algorithms with different key sizes. The RSA technique was selected since it is the most extensively used digital signature algorithm, whereas ECDSA is a well-known alternative to RSA because of its smaller key and signature size. One message per key pair is signed using the one-time signature (OTS) technique. It allows for larger signature sizes and is easy to compute.

4. The System Model

In a wireless sensor network, a sensor-based monitoring system is built that utilizes digital signatures to authenticate sensor nodes. It uses a linear programming approach to calculate the upper bound of the system's lifetime and create an assignment matrix. The assignment matrix is factored into a series of schedule matrices using the factorization algorithm and the k-matching approach to reach the system's maximum lifetime. These schedule matrices indicate the group of active sensors and the route to transfer the acquired data to the base station. In this model digital signature is used only for non-repudiation purpose and

signature verification is done by the base station only. Table I presents the terminology used for linear programming problems.

Table I

Terminology Used For Formulation of Lpp

Term	Description
f_{ij}	Delivery of data packets from node-*i* to node-*j*
B	Base Station
S	Group of sensors, |S|=n
T	Group of spots, |T|=m
k	Number of sensors require to monitor one single spot at any time
S(j)	Group of sensors that monitor spots-*j, j=1, 2, ……., m*
T(i)	Group of spots that are within the monitoring range of sensor-*i,i=1,2,……,n*
N(i)	Group of neighbor node of sensor-*i*
E_i	Energy budget of sensor-*i, i=1, 2……..., n*
d_{ij}	Distance between sensor node-*i* and node-*j, i,j=1,2,……n,B*
R	Data generation rate of a sensor while monitoring a spot
$\mathbf{E}^{s}$	Energy needed to sense one unit of data
$\mathbf{E}^{t}$	Energy needed to transmit one unit of data
$\mathbf{E}^{r}$	Energy needed to receive one unit of data
t_{wsn}	Life time of monitoring system
z_{ij}	Total amount of time sensor-*i* monitoring spot-*j*
$\mathbf{O}_{f}$	Signature length of a digital signature algorithm
$\mathbf{O}_{e}$	The amount of energy required by a digital signature algorithm to sign one unit of data.
r	Signing rate
E^{elec}	Electrical energy
ε^{amp}	Amplifier energy
α	Path loss exponent

The solution is divided into three parts:

- Using a linear programming approach, determine the upper bound of the life-time of the system and frame an assignment matrix from the computed value of z_{ij}.
- Factorize the assignment matrix into a succession of schedule matrices in such a way that the maximal life time can be achieved.
- Find the optimal path of data flow from node-*i* to node-*j* using *k*-matching algorithm.

S (i) and S(j) may be overlap for i ≠ j
T (i) and T (j) may be overlap for i ≠ j

Linear programing formulation for maximize the lifetime of the system while applying digital signatures.

Max t_{wsn}

Subject to:

$$\sum_{i \in s(i)} z_{i,j} = kt_{wsn}, \forall_j \in T \tag{1}$$

To monitor each target-j in the group of targets (T), *k*-sensors are required; the total time target-j is under supervision is k-times the system's lifetime, according to equation (1).

$$\sum_{j \in T(i)} z_{i,j} \leq t_{wsn}, \forall_i \in S \tag{2}$$

According to equation (2), the total working time of each sensor-*i* in S should not exceed the system's lifetime.

$$E^s \times R \times r \times O_e \sum_{j \in T(i)} z_{i,j} + E^t \sum_{j \in N(i) \cup \{B\}} f_{i,j} + E^r \sum_{j \in \forall_i \in V(i)} f_{j,i} \leq E_i, \forall_i \in S \tag{3}$$

(Conservation of energy)

Equation (3) states that a sensor node's overall energy cost must not excel its initial energy reserve. The cost of sensing data (i.e., monitoring targets), the cost of communicating data (which varies depending on the transmission distance), and the cost of receiving the data are the three components of energy consumption in a sensor monitoring system.

$$R \times r \times O_f \sum_{j \in T(i)} z_{i,j} + \sum_{j \in N(i)} f_{j,i} = \sum_{j \in N(i) \cup \{B\}} f_{i,j}, \forall_i \in S \tag{4}$$

(Conservation of data flow)

Flow conservation is represented by equation (4) that for each sensor-*i* in S, the total volume of data sensed and received should be equal to the total volume of data transmitted.

$$z_{i,j} \geq 0, f_{i,j} \geq 0 \tag{5}$$

(Non-negative data flow)

It is a common LP formulation, in which the objective is to maximize t_{wsn} and $z_{i,j}$, are the decision variables $1 \leq i \leq n$, *and* $1 \leq j \leq m$ and f_{ij}; *i j=1, 2,..., n, B*are variables of real numbers. As a result, the optimal outcomes of z_{ij}, f_{ij} and t_{wsn} can be computed in polynomial-time.

The value of $z_{i,j}$ obtained from linear programming can be represented as assignment matrix(A) as:

$$A_{n\times m} = \begin{bmatrix} z_{1,1} & z_{1,2} & \ldots & z_{1,m} \\ z_{2,1} & z_{2,2} & \ldots & z_{2,m} \\ \ldots & \ldots & \ldots & \ldots \\ z_{n,1} & z_{n,2} & \ldots & z_{n,m} \end{bmatrix} \tag{6}$$

The assignment matrix reveals two essential elements as:

- Summation of each column elements is equal to *k*-times of the life-time of the system ($k \times t_{wsn}$).
- Summation of each row elements is equal to the life-time of the system (t_{wsn}).

A. *Factorization of Assignment Matrix*

The life-time of sensor monitoring system can be split into a series of schedule matrix. Each schedule matrix contains a group of sensors, schedule to track their respective spots. A subset of sensors is scheduled in one session, followed by another subset of sensors in the next session, and so on. Each column contains exactly *k*-non zero entries depicting each spot should be monitored by exactly *k*-sensor in one session.

$$\begin{bmatrix} z_{1,1} & z_{1,2} & \ldots & z_{1,m} \\ z_{2,1} & z_{2,2} & \ldots & z_{2,m} \\ \ldots & \ldots & \ldots & \ldots \\ z_{n,1} & z_{n,2} & \ldots & z_{n,m} \end{bmatrix} = \begin{bmatrix} 0 & c_1 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ c_1 & c_1 & \ldots & c_1 \end{bmatrix} + \begin{bmatrix} c_2 & c_2 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & c_2 & \ldots & c_2 \end{bmatrix} + \ldots + \begin{bmatrix} 0 & c_t & \ldots & 0 \\ c_t & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & c_t & \ldots & c_t \end{bmatrix}$$

(7)

The breakdown of the workload matrix into a series of schedule matrices is represented by Equation (7). Each column contains exactly k positive values, suggesting that each target should be watched by k sensors, and each row contains just one positive number, indicating that each sensor can only monitor one target at a time and that there is no switching between targets throughout a session. The zeros make up the rest of the matrix. Furthermore, this matrix's nonzero components all have the same value, which symbolises the session's duration. The symbolic representation of schedule matrix is shown by equation (8).

$$A = A_1 + A_2 + ... + A_t \tag{8}$$

Where Ci = Time duration of session-i, t = Number of sessions, Ai = Schedule matrix, $i = 1, 2, \ldots, t$

Since, $n \geq km$ (No. of sensor is either greater than km or equal to km). In this paper $n=km$ is taken into account. According to equation (1) and (2) of LP formulation, the column sum (C_j) and row sum (R_i) are represented by equation (9) and (10) respectively.

$$C_j = kt_{wsn}, j=1,2,3\ldots\ldots\ldots\ldots\ldots\ldots\ldots m \tag{9}$$

$$R_i \leq t_{wsn}, i=1, 2, 3\ldots\ldots\ldots\ldots\ldots\ldots n \tag{10}$$

It is noted that the column-sum (Cj) of workload matrix equals to the row-sum (Ri). Therefore, the assignment matrix (A) is used to derive the equation (11) as:

$$\sum_{i=1}^{n} R_i = \sum_{j=1}^{m} C_j = mkt_{wsn}$$

Since, $n=km$

$$\sum_{i=1}^{n} R_i = \sum_{j=1}^{m} C_j = nt_{wsn} \tag{11}$$

Equation (12) is formed by combining equations (10) and (11).

$$R_i = t_{wsn}, i=1, 2, 3\ldots\ldots n \tag{12}$$

The possibility of factorization of the assignment matrix into a series of schedule matrices is generated by equations (9 and 12). The assignment matrix (A_{nxm}) can be represented by a bi-graph $G(S \cup T, E)$, with one set containing a group of sensors $S= \{s_1, s_2, s_3 \ldots s_n\}$ and other set contains a group of spots $T= \{t_1, t_2, t_3 \ldots t_m\}$. There is an edge between s_i to t_j for every non-zero elements z_{ij} in assignment matrix (A_{nxm}) and weight of an edge is represented as: $z_{i,j}$.

Each row of a session-i of the schedule matrix contains one entry with a non-zero value, and each column has exactly k-non-zero entries specifying the k-sensor monitoring this spot. This can be represented by k-sensors corresponding to a single point in the bi-graph (G). As a result, the problem of determining a series of schedule matrices is transformed into the problem of determining k-matching in a graph (G).

To find the series of schedule matrices for a given value of S, T, and k, the following conditions must be met.

- Every single sensor can monitor at most one spot at one time.
- Every single spot must be monitored by k-sensor at one time, where $k \geq 1$.

FillMatrix Algorithm

FillMatrix(Assignment matrix A_{nxm})

Input: Assignment matrix A_{nxm}.

Output: A matrix filled with entries w_{pxq}.

Begin:

$p = n+n\%k$; $q=(n+n\%k)/k$; $R'_i = t_{wsn} - R_i$ *for* $i=1$ to p;

$C'_j = k\ t_{wsn}$ *for* $j=1$ *to* $q-m$; $i=1; j=1$;

while($i \leq p$ && $j \leq q-m$) do

if($C'_j > R'_i$)

$z_{ij} = R'_i$; $z_{ik}=0$ *for* $k=j+1$ *to* $q-m$; $C'_j = C'_j - z_{ij}$; $i=i+1$;

else if($R'_i > C'_j$)

$z_{ij} = C'_j$; $z_{kj}=0$ *for* $k=i+1$ *to* p; $R'_i = R'_i - z_{ij}$; $j=j+1$;

else

$z_{ij} = R'_i$; $z_{ik}=0$ *for* $k=j+1$ *to* $q-m$; $z_{kj}=0$ *for* $k=i+1$ *to* p;

$C'_j = C'_j - z_{ij}$; $i=i+1$; $j=j+1$;

End if;

End while;

K-Matching Algorithm

K-Match (Assignment matrix A_{nxm})

Input: Assignment matrix A_{nxm}.

Output: A schedule matrix A_i.

Begin:

Step-1: Represent A_{nxm} as a bi-graph $G(S \cup T, E)$

Step-2: Convert graph G to graph G_k by substituting each spot in T by k- replica spots

Step-3: Merge replica spots by optimization algorithm for perfect matches and find a schedule matrix A_i

End;

Factorization Algorithm

Fact (Assignment matrix A_{nxm})

Input: Assignment matrix A_{nxm}.

Output: Series of schedule matrices $A_1, A_2, A_3 \ldots A_t$.

Begin:

If $n>km$ then

Call *FillMatrix algorithm* on A_{nxm} *to get* w_{pxq},*where* $p=n+n\%k$, $q=(n+n\%k)/k$

Make a bipartite Graph G from $w_{pxq.}$

While there exists an edge in G do

Call *K-Match* (A_{nxm}) to create a schedule matrix A_i;

Subtract A_i from w_{pxq} and delete edges with a weight of 0 in G

End while;

Output: $w_{pxq} = A_1+A_2+A_3+\ldots. +A_t$.

End if;

Table II

Signature Parameters

Energy type	Value in mj
Electronic Energy (E^{elec})	50×10^{-6}
Amplifier Energy (ε^{amp})	100×10^{-9}
Sensor Energy (E_i)	243×10^{3}

Table III

Energy Parameters

Algorithms	Key Length(bits)	Size of Signature (O_f)(bits)	Costs of Energy (O_e) (mj)
Proposed	55	110	33.53
OTS	80	3120	0
RSA	1024	1024	304
ECDSA	160	320	22.82
OTS	112	6160	0
RSA	2048	2048	2302.7
ECDSA	224	448	61.54

5. Experimental Setup

The relative performance of the proposed scheme has been compared to that of existing solutions; all digital signature algorithms are considered to generate data at the same rate. Considering α=2 for the free space model, α=4 for the multipath fading channel, $E^s = E^r = E^{elec} = 50x10^{-6}$mj and distance between adjacent node ($d_{i,j}$)=1000cm. Transmitting energy (E^t)= $E^{elec} + \varepsilon^{amp}(dij)^{\alpha} = 50x10^{-6}$mj $+100x10^{-9}x(1000)^2 = 10005x10^{-5}$mj for propagation model in free space and (Et)=100050mj for channel with multipath fading.

Typically, compressed images are 25kb or 25344 bits in size. Therefore, signing rate *r=1/25344* and sensing data rate *R=1* is chosen for simulation. Matlab IDE Version R2020A is being used for simulation. Figure 1 depicts the pictorial demonstration of linear topology sensor network with a base station (BS), five sensors, and three spots. The experiment is carried out

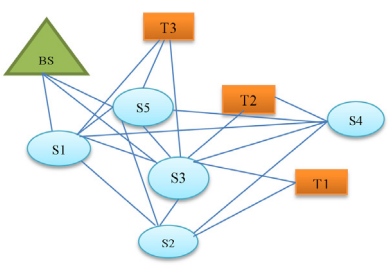

Figure 1

Linear network with 6-sensors and 3-spots

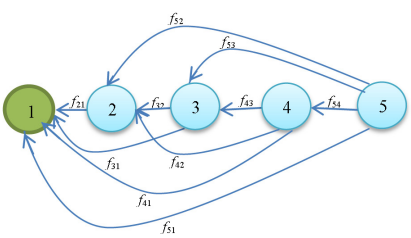

Figure 2

Illustrations of linear sensor network

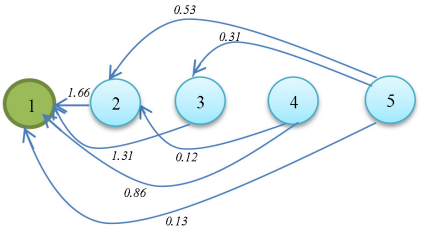

Figure 3

Flow balance with 5-node for α = 2

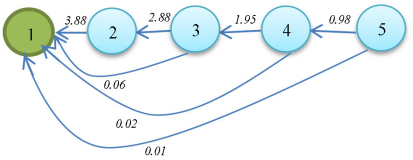

Figure 4

Flow balance with 5-node for α = 4

on a linear sensor network with 5-node as illustrated in Figure 2. Node-1 is the base station. Figure 3-4 show the energy efficient path for α=2 and α=4 respectively. The parameters of a signature are listed in Table II and Table III presents the energy parameters used for this experiment. Table IV shows the calculated parametric value for proposed, OTS-80, RSA-1024, ECDSA-160, OTS-112, RSA-2048 and ECDSA-224.

Table IV

Parameters for Proposed Model, OTS-80, RSA-1024, ECDSA-160, OTS-112, RSA-2048 AND ECDSA-224

Algorithms	O_e (mj)	O_f (bits)	r	R	R×r×O_f	R×r×O_e	t_{wsn}
Proposed	19.05	433	1/25344	1	0.0170	0.00075	45.61
OTS-80	0	3120	1/25344	1	0.1231	0	32.69
RSA-1024	304	1024	1/25344	1	0.04040	0.01199	17.56
ECDSA-160	22.82	320	1/25344	1	0.01262	0.00090	22.46
OTS-112	0	6160	1/25344	1	0.24305	0	24.52
RSA-2048	2302.7	2048	1/25344	1	0.08080	0.09085	10.84
ECDSA-224	61.54	448	1/25344	1	0.01767	0.00242	20.12

6. Simulation and Analysis

The initial energy reserved (E_i) for the sensor is 243x103mj, path loss exponent α=2 for free space model and α=4 for multi-path fading is taken into account for simulation. The simulation is performed by considering the five parameters as: (i)the number of sensor nodes in the network (ii) the maximal transmission range (iii)the monitoring range (iv)the number of sensors needed by each spot and (v) the change in signing rate for

path loss exponent α=2 and α=4. The life-time of WSN has been analyzed for proposed algorithm along with another digital signature algorithm. The proposed system runs the *k*-matching algorithm in the network topology graph and calculates a schedule matrix for all active sensors to track the spots. For every schedule matrix in the session the minimum energy consumption route from each sensor to base station are computed. If any sensor in the path drains out its energy, then remove it from the path and run the *k*-matching algorithm again and find a new schedule matrix and designated path. The *k*-matching algorithm runs until all the spots get covered and path to base station are calculated. Figure 5 and Figure 6 shows the life-time of WSN for proposed model and other digital signature algorithms (OTS-80, OTS-112, RSA-1024, RSA-2024, ECDSA-160 and ECDSA-224) against change in monitoring range and maximal transmission range respectively. Experimental results show that the lifetime of the system increases rapidly while increasing the monitoring range. More numbers of sensor are capable to cover the multiple spots, while increasing the monitoring range. This allows more flexibility in scheduling sensors and achieving maximum life-time. Furthermore, it can be seen that increasing the maximum transmission range enhances the lifetime of the WSN. Usually monitoring range is shorter than the transmission range of sensors. There is always a challenge for maximizing the life-time of WSN; because some spots are not monitored by sufficient sensors this often results in quick breakdown of the monitoring system. Figure 7 shows how the life time of WSN affected while growing the number of sensor nodes placed in the region. As increases the deployment of sensors in a region, density of the sensor node becomes higher and there are greater chances of a spot to be in the monitoring range of several sensors. Simultaneously a sensor can have more neighbors to find energy efficient path to forward data to base station. Therefore, the system gains more advantages by optimizing the schedule matrix, and the life-time of WSN is increases as increases the number of sensor nodes. When compared to existing digital signature algorithms (OTS-80, OTS-112, RSA-1024, RSA-2024, ECDSA-160 and ECDSA-224), the lifetime of WSN in the proposed solution increases rapidly.

Figure 8 shows the life time of WSN for proposed model along with other digital signature algorithms (OTS-80, OTS-112, RSA-1024, RSA-2024, ECDSA-160 and ECDSA-224) against the number of sensors needed by each spot (*k*) throughout the monitoring. The life-time of the system decrease while increasing the value of *k*. As the value of *k* increase, more sensors are involved to monitor a particular spot. However, the proposed

system shows the significant improvement in lifetime compared to other signature algorithms.

The *k*-matching algorithm is executed while adjusting the signing rate and the scheduling matrix is created to see how signature rate influences the lifetime of the WSN. Figure 9-12 depicts the lifetime of the monitoring system with the proposed algorithm, OTS-80, OTS-112, RSA-1024, RSA-2024, ECDSA-160 and ECDSA-224 for three different signing rates. Transmitting energy (E^t) strengthen by second power (α=2) and fourth power (α=4) of node-to-node distance. By keeping all other variables constant; it is observed that changing in signing rate and its impact on life-time vary accordingly as per algorithm is being used. By reducing the signing rate by a factor of ten, the lifetime of the proposed model increases 1.3 times as compared to RSA-1024, 1.5 times to RSA-2048, and 2.3 times to ECDSA-160 and ECDSA-224, although the improvements are minimal for OTS-80 and OTS-112.

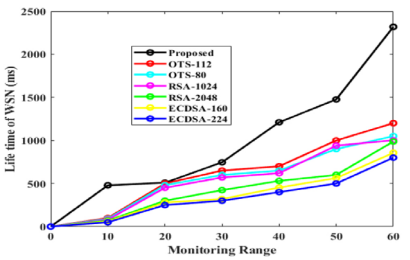

Figure 5

The life-time of WSN while changing the monitoring range

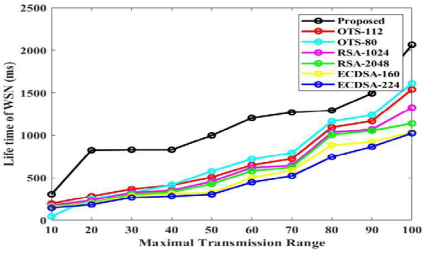

Figure 6

The life-time of WSN with while changing the maximal transmission range

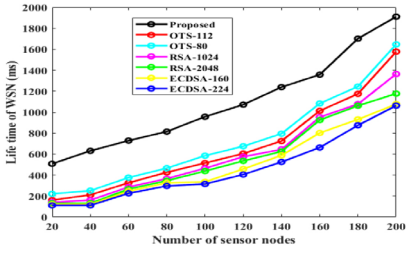

Figure 7

The life-time of WSN while increasing the number of nodes

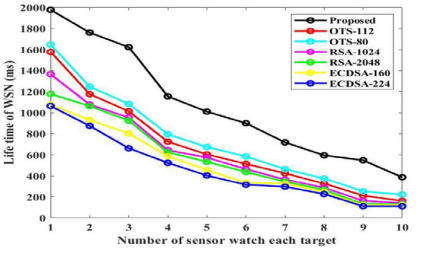

Figure 8

The lifetime of WSN while increasing the value of *k*

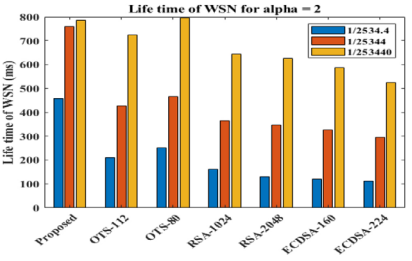

Figure 9

The life-time of WSN while changing the value of signing rate(*r*) for α=2

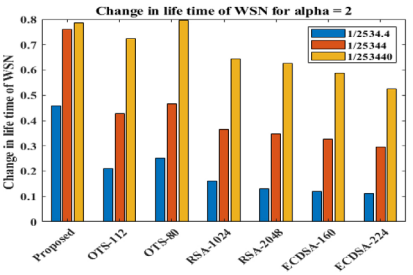

Figure 10

The change in life-time of WSN while changing the value of signing rate(*r*) for α=2

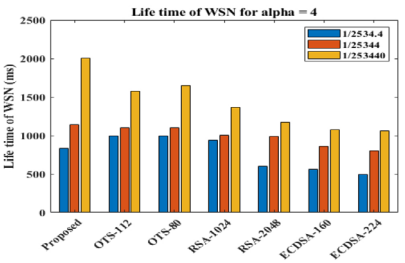

Figure 11

The life-time of WSN while changing the value of signing rate(*r*) for α=4

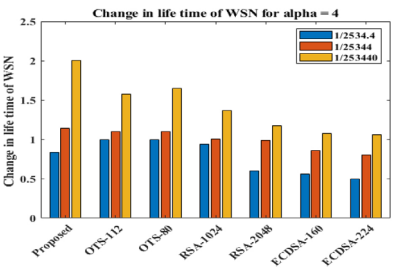

Figure 12

The change in life-time of WSN while changing the value of signing rate(*r*) for α=4

7. Limitations

- Some targets are not monitored by sufficient sensors, and this often results in a quick breakdown of the monitoring system.
- In multi-hope scenarios, digital signatures are used. Due to network interface costs and waiting time, WSN adds extra overhead. As a result, the security protocol should be built to reduce the delay time as much as possible.
- When the digital signature algorithm is used, WSN's lifetime is reduced.
- When the batteries in the sensor nodes are low, the running digital signature-based system requires more energy.

8. Conclusions

This paper explains the lifetime of sensor monitoring system using schedule matrix while employing digital signatures as a security service. The LP modal framework has been formulated and by using this modal a comprehensive simulation and analysis has been performed to measure the impact of various parameters on life time of sensor monitoring system. The proposed solution is divided in three parts; finding the maximal life time of the system and assignment matrix using linear programing problem, factoring the assignment matrix into a series of schedule matrix using *k*-matching scheme, and find an optimal path for each schedule matrix. These optimal paths specify the more energy efficient path from a sensor node to base station. Simulation and analysis are carried out against five parameters as: (i) the number of sensors in the network (ii) the maximal transmission range (iii) the monitoring range (iv) the number of sensors needed by each spot and (v) the changing in signing rate.

Acknowledgement

S. K. S. is financially supported by the University Grants Commission (UGC) New Delhi, India.

References

[1] Pankaj Kumar and Saurabh Kumar Sharma, "An Empirical Evaluation of Various Digital Signature Scheme in Wireless Sensor Network," *IETE-Technical Review,* vol. 8, pp. 1247-1256, Jun 2021.

[2] Krishna, A.V. Narayana, A.H. Narayana and K. Madhura Vani, "Fully homomorphic encryption with matrix based digital signature standard," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 20, no. 2, pp.439-444, 2017.

[3] S. Mukhopadhyay, D. Panigrahi, S. Dey, "Data aware, low-cost error correction for wireless sensor networks," *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*, vol. 4, pp. 2492–2497, 2004.

[4] V. Raghunathan, C. Schurgers, S. Park, M.B. Srivastava, "Energy-aware wireless micro sensor networks," *IEEE Signal Processing Magazine,* vol. 19, no. 2, pp. 40–50, 2002.

[5] I. Verbauwhede, A. Hodjat, D. Hwang, B.-C. Lai, "Security for ambient intelligent systems," Ambient Intelligence, pp. 199–221, 2005.

[6] B. Tavli, M. Kayaalp, O. Ceylan, I.E. Bagci, "Data processing and communication strategies for life-time optimization in wireless sensor networks," *AEU –International Journal of Electronics and Communications,* vol. 64, no. 10, pp. 992–998, 2010.

[7] B. Tavli, I.E. Bagci, O. Ceylan, "Optimal data compression and forwarding in wireless sensor networks," *IEEE Communications Letters,* vol. 14, no. 5, pp. 408–410, 2010.

[8] M. Bhardwaj, T. Garnett and A. Chandrakasan, "Upper Bounds on the Life-time of Sensor Networks," *Proc. IEEE Int'l Conf. Comm.*, vol. 3, pp. 785-790, 2001.

[9] L.B. Ruiz et al., "Scheduling Nodes in Wireless Sensor Networks: A Voronoi Approach," *Proc. 28th IEEE Conf. Local Computer Networks (LCN '03),* pp. 423-429, Oct. 2003.

[10] R.A. Brualdi and H.J. Ryser, "Combinatorial Matrix Theory,", no. 39, pp. 9-10, 1991.

[11] M.L. Sichitiu, "Cross-Layer Scheduling for Power Efficiency in Wireless Sensor Networks," *Proc. IEEE INFOCOM*, vol. 3, pp. 1740-1750, 2004.

[12] D. Tian and N.D. Georganas, "A Coverage-Preserving Node Scheduling Scheme for Large Wireless Sensor Networks," *Proc. First ACM Int'l Workshop Wireless Sensor Networks and Applications*, pp. 32-41, 2002.

[13] L. Sang, A. Arora, "Spatial signatures for lightweight security in wireless sensor networks," *Proceedings of the IEEE Conference on Computer Communications (INFOCOM),* pp. 2137–2145, 2008.

[14] S. Seys, B. Preneel, "Power consumption evaluation of efficient digital signature schemes for low power devices," *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob),* vol. 1, pp. 79–86, 2005.

[15] J.H. Chang, L. Tassiulas, "Maximum life-time routing in wireless sensor networks," *IEEE/ACM Transactions on Networking,* vol. 12, no. 4, pp. 609–619, 2004.

[16] S.C. Ergen, P. Varaiya, "On multi-hop routing for energy efficiency," *IEEE Communications Letters,* vol. 9, no. 10, pp. 880–881, 2005.

[17] H. Liu, X. Jia, P.-J. Wan, "Maximal Life-time Scheduling for Sensor monitoring system with *K*-Sensor to One Spot," *IEEE Transactions on Parallel and Distributed System,* vol. 17, no.12, pp. 1526-1536, Desc. 2006.

[18] K. Bicakci, I. E. Bagci, B. Tavli, "Communication/computation trade-offs for prolonging network life-time in wireless sensor networks: The case of digital signatures," *TOBB University of Economics and Technology,* Sogutozu Cad, Sogutozu, TR-06560, Ankara, Turkey, no. 188, pp. 44-63, 2012.

[19] H K Kalita and A Kar, "Key Management in Secure Self Organized Wireless Sensor Net-work: A New Approach," *International Conference and Workshop on Emerging Trends in Technology,* pp. 865-870, 2011.

[20] Abdullah Al-Mahmud, Rumana Akhtar, "Secure Sensor Node Authentication in Wireless Sensor Networks," *International Journal of Computer Applications*, vol. 46, no. 4, pp. 10-17, May 2012.

[21] K.Ren, S Yu, W.Lou and Y Zang, "Multi-User Broadcast Authenticationin WSN," *IEEE Transaction on Vehicular Technology*, vol. 99, pp.1-10, 2009.

[22] A. Abror, Lee Young-Koo Lee Sungyoung , "Simple Hash Based Message Authen-tication Scheme for WSN," Work supported by IT & R & D program of MKE/KEIT, pp. 982-986, 2009.

[23] Oscar Delgado-Mohatar, Amparo Fster-Sabater, and Jos M. Sierra, "Alight-weight authen-tication scheme for wireless sensor networks," *AdHoc Networks, Elsevier*, vol. 9, no. 5, pp. 727-735, July 2011.

[24] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: security protocols for sensor networks," *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom '01),* Rome, Italy, vol. 8, no. 5, pp. 189–199, July 2001.

[25] Y. Zhou and Y. Fang, "WSN09-1: BABRA: batch-based broadcast authentication in wireless sensor networks," *Proceedings of the 49th Annual IEEE Global Telecommunications Conference (GLOBECOM '06),* San Francisco, Calif, USA, pp. 1–5, Dec. 2006.

[26] X. Cao, W. Kou, L. Dang, and B. Zhao, "IMBAS: identity based multi-user broadcast authentication in wireless sensor networks," *Computer Communications,* vol. 31, no. 4, pp. 659–667, 2008.

Received March, 2022

Revised August, 2022