A Novel Trust based node integrity verification and privacy preservingmodel for Dynamic WSNs

Seshagiri Rao Ganta[1], Dr N Naga Malleswara Rao[2]

[1]Research Scholar, Department of CSE,
University College of Engineering, Acharya Nagarjuna University, Guntur, India
[2]Professor, Department of Information Technology, RVR and JC College of Engineering, Guntur, India.

Abstract:

Wireless sensor networks (WSNs) plays a vital role in many real-time applications due to its topology structure, network size and communication. Data privacy, node path planning and integrity are the essential factors that optimizes the network efficiency and trust. Since, most of the traditional WSN path planning are independent of integrity and node trust computation, it is difficult to provide privacy and robust path planning in large WSNs. In order to overcome these issues, a hybrid trust-based node integrity verification and privacy preserving model is implemented for the dynamic WSNs. In this model, a hybrid ACO based node trust probability and path planning is proposed along with new local update and global update measures. Experimental results proved that the present trust based model has better runtime, hash variation and privacy preserving metrics than the traditional WSNs cluster based authentication protocols.

Keywords: WSNs, hash value, ACO, encryption.

1. Introduction

Wireless sensor networks (WSNs) are designed and implemented to transfer sensitive data during the process of area monitoring and infrastructure monitoring. The whole network is a collection of very small smart devices which are also known as sensor nodes. The authentication and security in the wireless networks have significant importance during the monitoring of different activities as well as environmental conditions. A single sensor node requires a limited number of iterations to compute the trustiness of the neighbour nodes and it is the main issue behind maximum energy consumption. In some cases, two neighbour sensor nodes are inactive for communication. In such cases, it is infeasible to compute the trustiness of the neighbour nodes. Applications of Wireless Sensor Networks (WSNs) are mostly implemented in real world scenarios, where human beings can't reach. It also includes huge numbers of randomly deployed sensor nodes. Wireless sensor networking is a recent networking paradigm to fit to the growing trend of broadband ubiquitous networking with its capability to support a wide range of application scenarios. End users can experience high speed service delivery as wireless sensor networks rely on multi-hop wireless backbone for data delivery without the need to deploy any fixed infrastructure. Typically sensor network is decentralized and compromise of wireless networking devices. That are within each other's range. Every node in a sensor network access a gateway and helps in routing packets across the sensor network. Various wireless network applications such as industrial monitoring, battlefield surveillance or disaster management systems, complete security of the whole network is very much essential in order to establish secure communication channel [4]. Different advanced cryptographic algorithms are proposed in order to ensure secure communication. But, still the system is vulnerable for some attacks like black hole attack, sink hole attack, DoS attack, and so on. To defend against these attacks, behaviour of sensor nodes in the network must be monitored appropriately. The monitoring process has the responsibility to distinguish between

trustworthy and un-trustworthy nodes of the network. During the communication process, trust factors are generally computed within certain interval. These trust factors are implemented in order to detect different types of malicious and vulnerable nodes. Node mobility is the major cause of topology modifications. Due to dynamic topology, it may lead to frequent link failures. Apart from this, some problems like re-authentication and communication with the certificate server may occur.

Resource constraints also greatly affect operating system and language features for WSN [5]. The lack of secondary storage systems precludes virtual memory architectures. Also, instead of deploying strictly layered software architectures, designers of system software often choose cross-layer designs to optimize resource efficiency. Optimal path planning frameworks for WSN nodes should support application designers to specify resource efficient and power-aware programs. However, more processing power only comes at a significant monetary price. Since all WSN require memory and typically rely on the finite energy reserves from a battery, this energy reserve is the limiting factor of the lifetime of a WSNsensornode. Also, many sensor node-node designs are severely constrained in fundamental computing resources, such as data memory and processor speeds. WSN typically lack some of the system resources typically found in traditional computing systems, such as secondary storage or arithmetic co-processors. This is particularly the case for nodes used in applications that require mass deployments of unobtrusive WSN, as these applications prompt small and low-cost sensor node-node designs. In addition to energy-aware hardware design, the node's system software must use the available memory efficiently and must avoid CPU-cycle intense operations, such as copying large amounts of memory or using floating-point arithmetic. Various software-design principles to save energy have been proposed. In many aspects WSN are reactive systems. Reactive systems are computer systems that are mainly driven by clone node events. Their progress as a computer system depends on external and internal events, which may occur unpredictably and unexpectedly at any time, in almost any order, and at any rate.

The path planning, clone node avoidance and security in the WSN networks have been given significant importance during the monitoring of different activities as well as environmental conditions [8]. It is difficult and a complex task to select and apply appropriate clone node avoidance model in the dynamic WSN networks. These nodes are usually powered by battery. Thus, these devices have restricted energy, computational and communication efficiency, bounded memory and processing speed. A discretized three-dimensional model is used in [9] built to plan paths for autonomous helicopters. The model has a hierarchical discretization and employs standard Dijkstra or A* graph search [10] an optimal solution at each hierarchy level.Planning for autonomous WSNs consists of a mechanism for generating decisions regarding action. For a planner to be effective, it must look both outward and inward. Not only it must be responsive to the environment within which the sensor node is operating, but the planner should also be sensitive to the evolving state of the sensor node itself. The WSN single path must be flyable and the WSN must not collide with any known clone nodes. Known clone nodes are represented using an elevation map because maps are readily available from the Geographical maps. Ideally, the clone node set is represented by a list of objects defined by polygonal boundaries so that path intersections can be determined easily. However, all terrain data is available in elevation grid format which requires incremental path checking.

Another important feature of this wireless sensor network is to relay the information those are transmitted from different nodes. By this, the network coverage can be enhanced. Both of these above mentioned nodes can be differentiated by two important characteristics, those are:- mobility and energy

consumption constraints. Sensor clients have restricted amount of energy than that of sensor routers. Hence, all of the functionalities those need large amount of computational time, bandwidth and memory are usually issues of sensor routers.

Mobility, flexibility and very high robustness can be achieved with the help of wireless sensor networks. Apart from this, the network coverage can also be enhanced with high scalability. There are vast numbers of applications of wireless sensor networks in the field of healthcare, enterprise networking, security surveillance, and so on. There have been extensive amount of research works carried out in order to ensure the security of wireless sensor networks. There are numbers of different efficient approaches by implementing which many attacks can be identified. Below are the severe issues those are found in the above mentioned research works.

1. Excessive packets are eliminated and those are not at all processed. Again, lower priority packets are also eliminated that may result packet loss.
2. The security protocol results huge control overhead because of cryptographic extension and acquisition delay.
3. These systems are not at all efficient and effective for huge numbers of nodes. It also results huge execution time.
4. Initial packet loss can be noticed because of probable selection of wormhole nodes.
5. In each and every case, these approaches results noticeable identification inaccuracy.

Passive as well as active attacks are found in wirelesssensor networks through wireless multi-hop communication. In case of wireless sensor networks, passive attacks may violate confidentiality. On the other hand, active attacks may violate authentication, integrity and non-repudiation. It is very much important to develop an efficient and effective security scheme in order to exchange the information. The traditional approaches are inefficient due to storage, energy and bandwidth restrictions. Therefore, there is necessity of an advanced authentication technique in order to overcome all the issues of wireless sensor networks.It also involves high speed wireless approaches and it has wide range. There are two major reasons for this authentication, those are:-

1. Each sensor domain is required to authenticate its every individual user in order to avoid fraudulent use of network resources.
2. Usually the authentication protocol is time consuming and infeasible in terms of costs. It involves the users, his home domain and his foreign domain also. On increasing the user base, the authentication signalling overhead is also increasing.
3. A new bilateral service level agreement is included among every pair of wireless sensor network domain in order to allow the process of user roaming.

Among all benefits of the above method, self-organization, minimum installation expenses, large-scale deployment, and fault-tolerance are significant ones. The above mentioned features are responsible to connect anywhere and anytime. Both sensor routers and sensor clients result poor security due to constrained computing and power supply.

Prior to the network access, every individual client is required to be authenticated with the help of a sensor access point. During the roaming of sensor access points, the client is required to be re-authenticated in order to access uninterrupted network services. In order to operate real-time applications and offer improved service, the

handover latency must not be greater than 50ms. The latest wireless sensor networking IEEE 802.16 requires 1000ms range in order to process Extensible Authentication Protocol (EAP) in case of a round trip among the client and the server.To decrease the latency at the time of roaming, numbers of different handover authentication protocols are introduced. The security issues are more complex in case of wireless sensor networks as compared to traditional wired and wireless networks.

2. Related Works

Goyal,et.al. Implemented ACO based elliptic curves and chaotic system to develop a new digital signature algorithm [6]. They integrated one-way hashing, 2D hyper-chaotic mapping with public key algorithm to form their new approach. Their algorithm prevents duplicate signature key attack. As the proposed algorithm is reliable, secure and simple it can be implemented in practical scenarios. In this section various works in the field of chaotic-based secure hash algorithms have been thoroughly studied. Their objectives are analysed and identified, along with empirical validations, pros and cons of each approach.

Wang et.al, proposed a collision resistant one-way hashing on path planning data[18]. In future, further works can be done to enhance some algorithms like MD4, MD5, SHA and, so on. They analysed various pre-existing techniques calculating storage patterns on WSNs, which led to some storage and sharing problems. It also resolves some other problems such as data encryption, boundary maintenance and data proof. All these operations are controlled and managed by view management scheme. Some of other advantages of this technique are: entity privacy, data availability and safe data sharing etc. Each and every sensor has its own view and also has a secure boundary.

MD5-ACO and MAC approaches are merged in order to put together their imperative properties and this newly developed method from the above integration is known as Role-Based Access Control (RBAC). The Discretionary Access Control (DAC) approach is sensor discretionary, whereas MAC technique is based on lattices. In order to overcome the disadvantages of RBAC approach, attribute based encryption techniques are proposed in [19]. Almost all access control approaches are dependent on PKI. According to the basic concept of public key based encryption, both the process of encryption and decryption are started executing by the sender's request for public key from Key Distribution Centre (KDC). The Public Key Infrastructure (PKI) authenticates the public by signing and transmits it to the requester. The public key is required by the sender in order to carry out the process of encryption successfully. The encrypted message is sent from sender to receiver in the unsecure WSNs channel. At the receiver's end, private key is needed for decryption of the cipher text message which is previously encrypted by the sender.

The method of ACO-IBE includes four algorithmic phases such as: setup, keygen, encryption and decryption. The setup algorithm produces the master key for receiver. Then, the receiver is required to validate his identity with the help of unique identities such as SSN; email to the Private Key Generator (PKG).The identity KeyGen (KG) algorithm is responsible for production of private key for receiver. In the process of encryption, the sender is aware of the identity of receiver (email). The sender utilizes the receiver's identity in order to execute the process of encryption efficiently. The receiver requires its own private key which is produced by PKG in order to decrypt the encrypted message. The major advantage of implementing WSNs based Identity Based Encryption (IBE) technique is that, the sensor is not required to communicate with Key Distribution Centre (KDC) for generating public key, because the sender is already aware of receiver's identity. Traditional key policy based attribute based encryption(KP-ABE) encryption technique resolves the issues of

WSNs based IBE approach. According to traditional ABE mechanism, the key policy of Attribute Based Encryption (ABE) is associated along with the sensor's identity. The overall process of attribute based encryption scheme includes four major algorithms needed to be executed, those are: Setup, KeyGen, Encryption and Decryption. Though WSNs has powerful and reliable server, there are numbers of threats both from outside and inside [20] which uses WSN's vulnerabilities. Hence, data confidentiality, data integrity, and data availability may be compromised. Untrusted service providers always hide such vulnerability of their system in order to maintain their reputations. Sometimes WSNs storage space is increased by removing least accessed data [21]. Many sensors as well as business organizations store their confidential data in WSNs.

If any attack happens, all the confidential data related to business organizations as well as sensors will be disclosed to the attacker [22].

- Key policy attribute based encryption is that it cannot decide WSNs sensor's decryptingdata which is in cipher form.
- Key policy attributes encryption can only choose limited attributes for access control mechanism.
- In cipher text policy, encryption schemes are difficult to represent the policies and manage authorized sensor attributes.
- Achieving the large attributes and key space are challenging factors in a WSNs environment.
- Traditional ABE schemes suffer with revocation issue in multiple WSNs servers.
- Identity based Encryption scheme suffers with one to many communication problems. That is, if the sender wants to share his data with multiple receivers, he must know all the receiver's identities.

P. Memarmoshrefi, et.al, proposed a novel attack detection approach for WSN path planning data. This technique completely depends upon an ant colony optimization system. One of the most common issues is security loop hole in the autonomous authentication process. The presence of pheromones is responsible for the representation of the trust level of nodes all across the certificate chain. The main limitation of this model is the overall scalability of the network need to be enhanced through the increase in numbers of nodes. Furthermore, this technique can be modified and extended in order to identify the certificate chains consisting of Sybil nodes with multiple identities.

Wang et.al, proposed [23] a cryptographic approach for protecting WSN path planning data in limited WSN networks. CP-ABE model was developed by Sahai [24].This model is based on the basic idea of cipher text associated with access control mechanism. Here, secret keys are also integrated with attributes. The process of decryption is permitted, when corresponding attributes satisfy its intended access policy. The whole working process of CP-ABE model is completely reverse of previously developed KP-ABE. As CP-ABE technique is more flexible as compared to other attribute-based encryption approaches, it can be easily implemented in wide range of applications. According to the KP-ABE approach, it was unable to control who will decrypt the cipher text which is considered as the major limitation of the said model. CP-ABE tried to overcome the mentioned issue of KP-ABE approach efficiently. Because of this feature, CP-ABE technique can be implemented in various real world applications successfully.

The above proposed model also has a severe drawback which restricts this scheme to be applied in enterprise scenarios. Due to less flexible nature of this model along with very low efficiency rate, it is not fit to

be implemented in enterprise applications. Attributes of single set are needed during the decryption process in order to successfully execute it. Users are meant to choose a particular attribute or a set of attributes out of that attribute set. Further research efforts have been made to resolve the detected issue of CP-ABE approach. Out of all developed solutions, CP-ASBE (Cipher text Policy Attribute Set Based Encryption) is identified as a perfect solution.

3. Proposed Model

In the proposed framework, each sensor client is initialized with unique sensor id as attribute in the dynamic WSN. Here, WS-1,WS-2..WS-n are the sensor client nodes in the WSN. These sensor nodes are used to initialize the sensor id and sensor data s shown in figure 1.

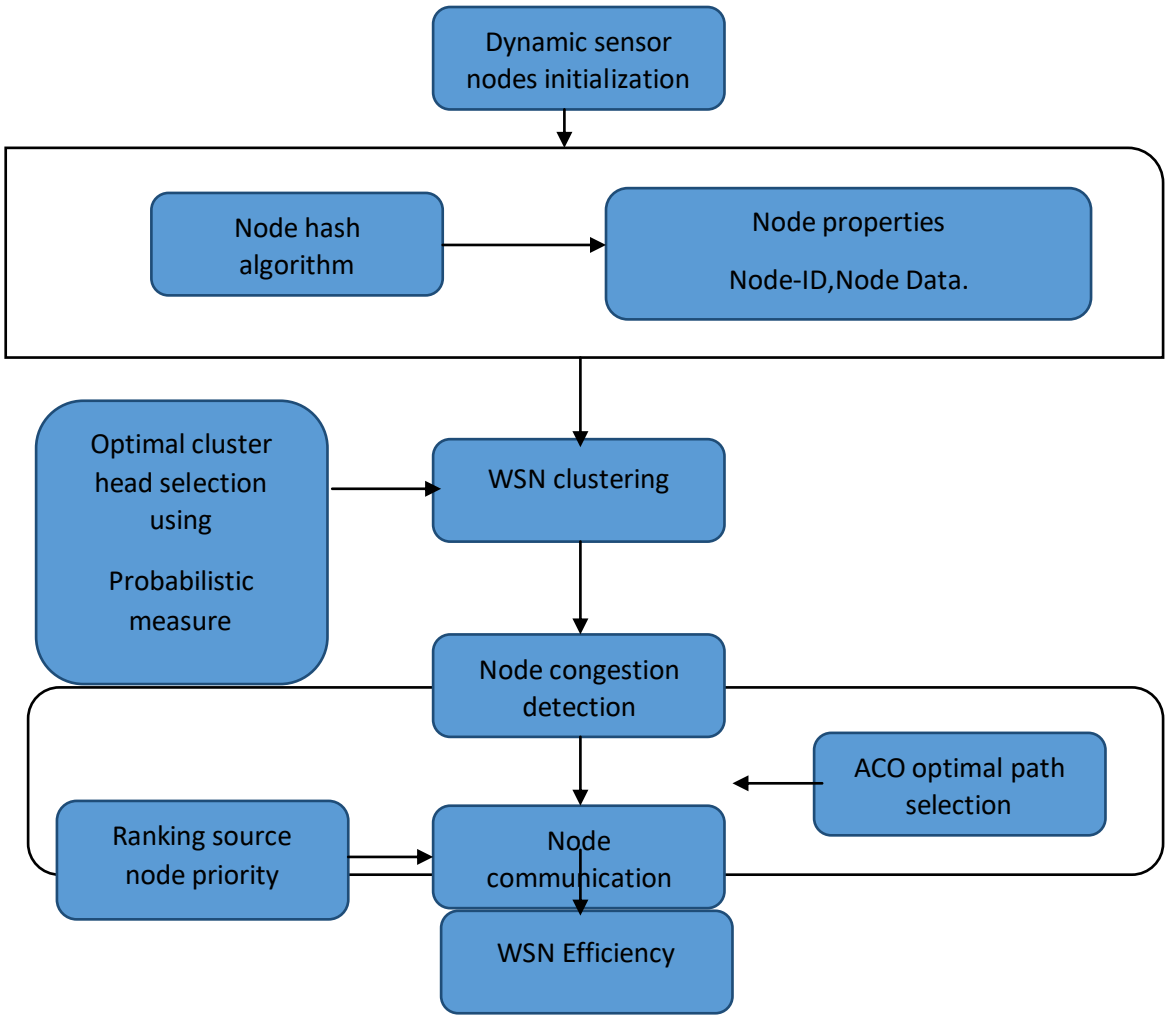

Figure 1: Proposed Framework

Here, the attribute list defines the names of the sensor identities for policies construction. Policy list is used to check the constraints on the attributes for data encryption and decryption process. In the proposed framework, a non-linear chaotic map is used to generate the randomization keys for encryption and decryption process as shown in the figure1. In this work, a dynamic chaotic key based cipher text policy attribute based encryption(CP-ABE) model is implemented to secure the communication data in the dynamic WSNs.

Proposed Algorithm 2: ChaoticNode Integrity Computation Algorithm

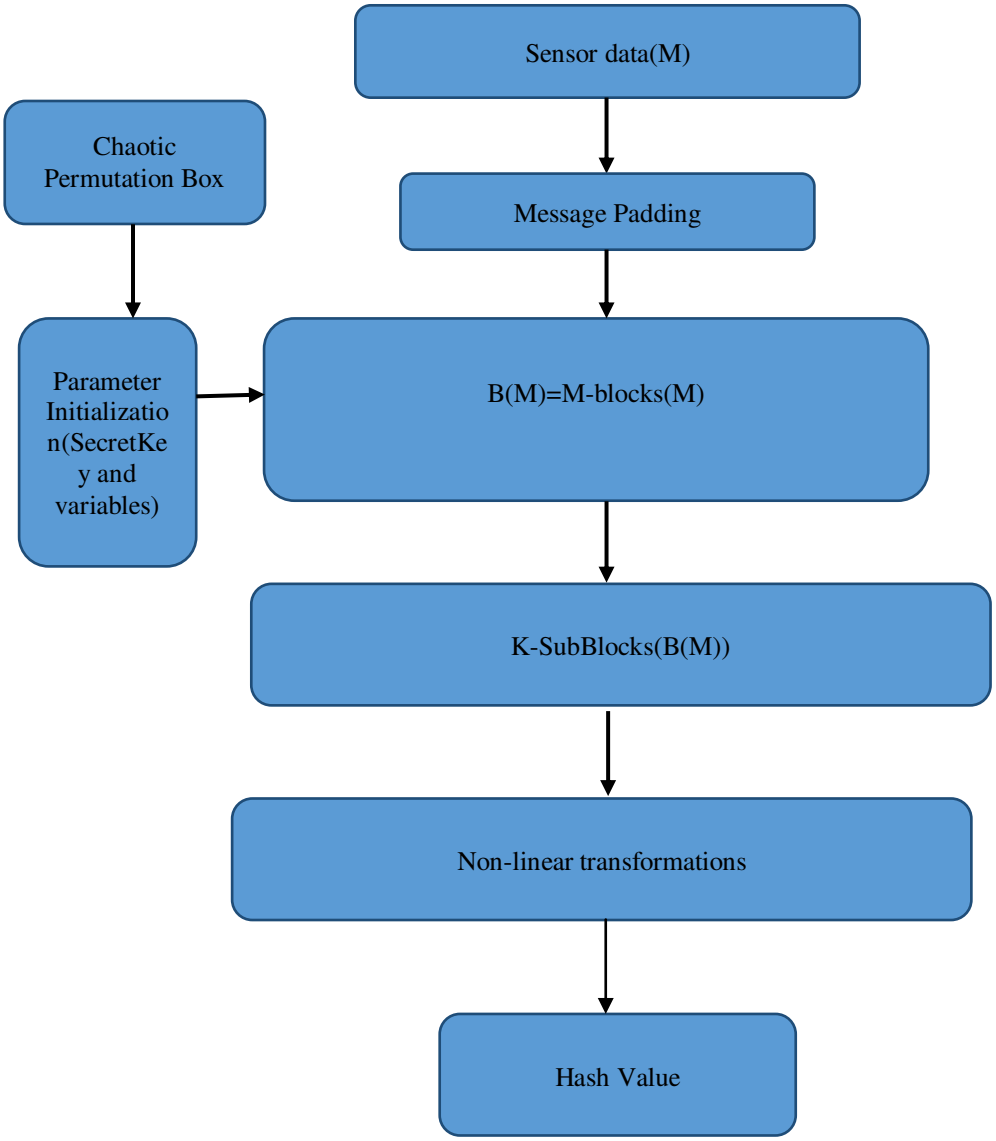

Figure 2: Trust based hash implementation in WSNs.

In the proposed model, a novel chaotic integrity verification algorithm is proposed to improve the performance of the wireless sensor clients in the dynamic WSNs. Figure 2, represents the proposed model architecture for integrity computational of the sensor clients. As shown in the figure, initially, each sensor client details and its data are taken as input to proposed integrity computation. If the size of the input message exceeds its hash size then the message is padded with 1 followed by zeros. Here, input message M is partitioned into blocks and then subblocks of size 32-bits each.

Computing Q using Secret Key matrix SK.

SK=[k1,k2..kn]

Using QR decomposition formula we have

SK=QR

$Q=SK.R^{-1}$

Here, the chaotic key generation is used to generate the sequence of high randomized values. These sequence of randomized chaotic values are used to initialize the permutation box and secret key in the integrity computation model.

Step 1: Input Sensor Client details M_ID and Data D, HashSize S, NR:Number of rounds.

Step 2: Message M=M_ID+D;

Step 3: Generate Secretkey SK using the dynamic chaotic permutation Box generated using the set of chaotic key generation.

Step 4: Divide the message M into S/8 blocks.

Step 5: while(|M|> S/8)

Do

Message Padding;

BlockProcess(M[S/8]);// step 6

Done

Step 6: BlockProcess

Partition the block into S/32 subblocks of 4 bytes each;

P[]=ParitionBlocks[S/32];

For i=0 to |P|

Do

for each round r in NR-1

Do

ProcessSubblock(P[i]) // step 7

Done

Done

Step 7: ProcessSubblock

For each byte in P[i]

Do

$U_1 = SK^T.\ [P[i].\ Rank(SK)]$

$$U_2 = \left(\frac{[Trace(Q).Rank(SK).\ (CBound(Poly(SK))]}{SumSquare(SK[i])\ /\ solve(Poly(cp))}\right)$$

$U_3 = \sum Eigen(Poly(Q))$ // sum **of eigen roots of polynomial equation**

$H[i] = U_1 \oplus U_2 \oplus U_3$

Done

Step 8: H=H[1]+H[2]+….H[NR]

In the proposed integrity computational algorithm, an improvement in the chaotic key generation and sub block processing are performed on the input sensor data. This algorithm is used to improve the high randomization and less computational time compared to the previous integrity verification algorithm.

Dynamic Chaotic CP-ABE Encryption Model:

Proposed integrity based encryption algorithm consists of four phases ie. Sensor Setup, sensor Encryption, sensor Chaotic Key generation, sensor decryption. Each phase and its mathematical formations are described below.

Phase1:Sensor setup: In this sensor setup phase, each sensor node initializes its own cyclic group parameters and chaotic

$$\text{Let } G_1, G_2, Z_p \text{ are cyclic group pairing elements.}$$
$$\text{Pubk} = \{H_{4096}(G_1), H_{4096}(G_2), g^{H_{4096}(Z_r)}\}$$
$$\text{Mk} = \{H_{4096}(Z_r), g^{H_{4096}(Z_r)}\}$$

Where R_n is the random field element in the cyclic group Z_n. Atree is the access tree structure.

Phase 2: Sensor data encryption: This phase takes a sensor attributes, sensor data as input and generates cipher text as output using the sensor public key and sensor integrity values.

$$\text{Ciphertext CB[i]}=\{\text{Atree}, R_n^{PB[i]}\}$$

Phase 3: Sensor Key Generation Phase : In this phase, sensor master key is used to generate the secret key. This secret is embedded with sensor integrity value for node authentication verification. The secret key is generated using the following formula.

$$\text{Sk} = \{\text{Attlist}, g, g.H_{4096}(\text{nodedata}), g^{H_{4096}(Z_r)}\}$$

Phase 4: Sensor key Decryption: In this phase, attribute list, cipher text and sensor integrity value are taken as input in order to decrypt the sensor data using the access tree structure.

The ACO technique was initially introduced by Marco Dorigo. He considered the actual behavioural patterns of real ants during food search process. They usually prefer the shortest route to their food from their home. Every ant leaves pheromone in the route and its trust is computed to each node for data communication. All the ants travelling in the shortest paths usually return source location earlier by following the same path than that of ants taking longer paths. Furthermore, the quantity of pheromone present in the shortest path is relatively more as compared to other paths. Hence, the new ants mostly follow this shortest path having more pheromone. The objective of this technique is to identify the optimal path among numbers of different other paths. The trust weigh is computed using the proposed probability measure and the nodes are remunerated through decreasing/ increasing of trust value. When the trust value becomes less than that of trust threshold, the node is considered as malicious. Therefore, this technique aims to achieve significant performance along with extended security.

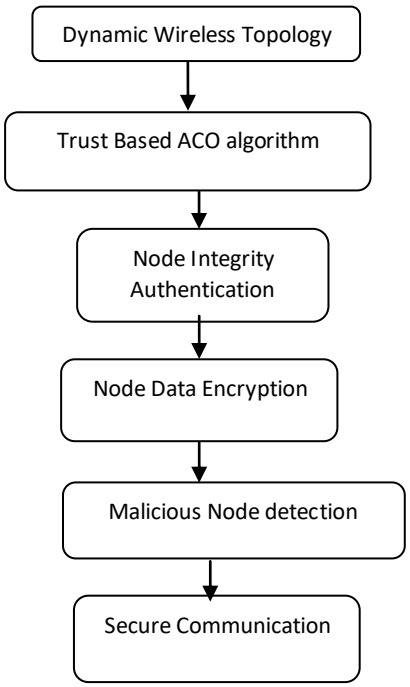

Figure 3: Overview of Proposed Model

The overview of the proposed model is shown in figure 3. In this model, initially a dynamic network topology is constructed using the proposed ACO algorithm. In this case, all the wireless nodes are initialized dynamically using the trust probability value. In the subsequent step, malicious nodes are discarded with the help of a probability trust and integrity verification process. After the initialization of the ACO based network topology, each node is authentication using the proposed integrity verification function. Each node is verified against its integrity value to detect the malicious clone node. Additionally, each sensor node data is encrypted using the ciphertext policy attribute-based encryption technique against the malicious attacks.

Algorithm 3: Optimized ACO algorithm

Step1:Initialization of ACO parameters

Step 2: To each ant in the number of ants
repeat
Initialize all ant solutions as true
Construct neighbour nodes and its paths until best solutions.

Nodes clustering steps:
To each node in the sensor network.
To each neighbour node to the current node.
Choose a new random centers ci
compute Lnorm distance by checking max {|x[i]-y[i]|, Log(Manhattan Distance)}
Repeat until optimal cluster heads are selected in WSN.

Compute Node pheromone as

Alpha: Pheromone weight

Beta: heuristic weight

$$NPh = \text{Min}(\text{Max}\_\text{Ph}, \text{Max}(\text{Min}\_\text{Ph}, \text{Ph}_c))$$

Ph_c : Current pheromone value

NH=1/distance(sn,nn);

$$D(\text{snode}, \text{neignode}) = \sqrt{(\text{snode.x} - \text{neignode.x})^2 + (\text{snode.y} - \text{neignode.y})^2}$$

$$\text{Newnode}(\alpha, \beta) = N_c.\text{getPh}(\text{neig})^{\alpha^2} * N_c.\text{getH}(\text{neig})^{\beta^2}$$

Trust probability is computed to each node for cluster head selection as

P_α : Pheromone weight
H_β : Heuristic weight

$$\text{TrustProb(TP)} = P(N_c)^{\sqrt{P_\alpha}} * H(N_c)^{\sqrt{H_\beta}}$$

Step 3: Update ant local and gobal best as.

$$\omega = ((1 + (1 - \eta) * (1 - P_c) * H_c) * P_c$$
$$\eta \in (0,1)$$

$$\text{LocalUpdate} : (1 - \eta) * (P_n) + \eta * \omega$$
$$\text{GlobalUpdate} : (1 - \rho) * (P_n) + \rho * (1 + P_n * H_n) P_n$$

Repeat to each node in the network.

Step 4: dynamic network topology is created with trusted paths.

4.Experimental Results

Experimental results are executed in Netbeans IDE tool using Java environment. In this experimental study, different initialization parameters such as number of sensor clients, malicious attack nodes, and number of iterations are taken as input for network setup.

WSN Setup:

In the sensor network setup, the simulation view is designed using the SWING library. Third party libraries such as Jama, JForm, Apache math, JSimulation are used to implement the proposed network topology.

The basic parameters used to setup the wireless sensor network is shown in table 1.

Parameter Name	Purpose
Sensor –ID	Sensor node identity
Data	Sensor node communication data
Nodes	Number of sensor nodes to setup in the wireless sensor topology
Malicious nodes	Number of malicious nodes initialized in the sensor network

WSN Initialization:

In the proposed algorithm, different colour nodes are initialized randomly in the WSNs as shown in Figure 3.

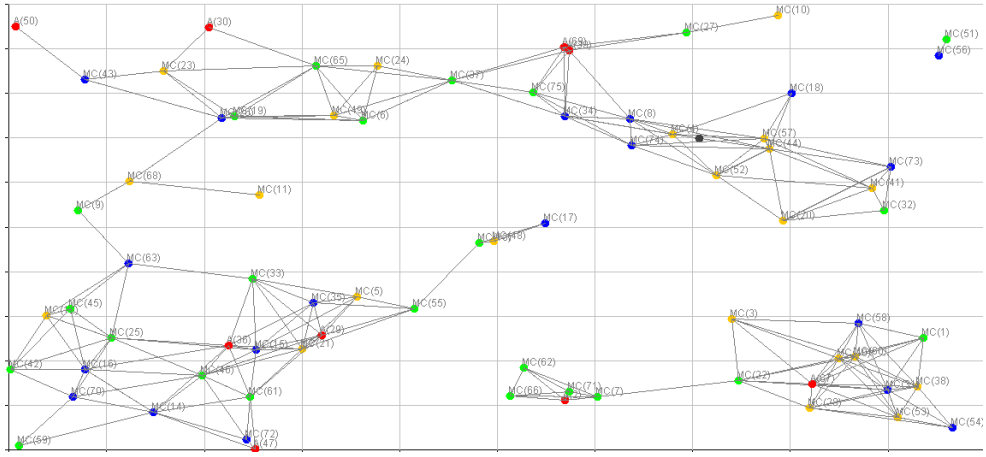

Figure 3: WSN initialization

The sensor network is initialized with sensor clients and malicious attack nodes. In the simulation, malicious attack nodes are represented in red colour and authorized sensor clients are represented in blue, green and yellow colours. For an efficient diffusion property, there should be 50 percent bit change in the hash value. The computed hash of the sensor node integrity is taken as binary form to check the change bits.

Table 1: Runtime(ms) computation of the proposed probabilistic kmeans and the existing algorithms

IterationNo	K-means	K-Means++	Fuzzy-CMeans	Trust-ProbabilisticKmeans
#1	3102.36	2675.34	2301.45	2097.11
#2	2899.96	2726.35	2438.06	1918.15
#3	3152.89	2631.19	2438.15	1989.44
#4	3045.14	2797.8	2218.93	1973.09
#5	3064.72	2458.2	2331.77	2092.7
#6	3169.33	2782.31	2472.55	2037.98
#7	2903.63	2475.47	2528.56	2077.7
#8	3016.13	2476.9	2163.13	1904.35
#9	2913.01	2546.44	2331.44	1982.58
#10	3213.27	2433.73	2462.56	2074.37
#11	2787.68	2456.76	2454.48	1910.82
#12	3056.63	2769	2169.85	1999.13
#13	3070.96	2407.2	2461.08	2099.21
#14	3167.46	2635.45	2144.02	2012.13
#15	3119.12	2362.24	2359.62	2050.03
#16	3188.92	2351.62	2432.86	2089.35
#17	3211.15	2845.34	2227.89	2027.26
#18	3124.47	2349.11	2397.6	2003.29
#19	3079.01	2470.13	2414.81	1988.43
#20	3063.2	2789.56	2530.85	1901.71

Table 1, describes the runtime(ms) computation of the traditional models to the present model in dynamic WSNs. From the table 1, it is observed that the present model has less runtime(ms) than the traditional models when the number of nodes is 50.

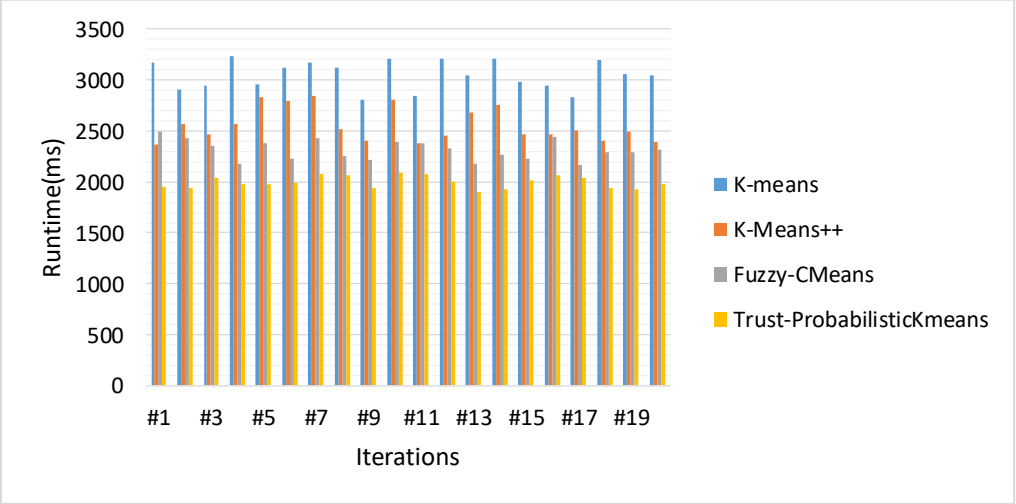

Figure 4: Runtime(ms) computation of the proposed probabilistic kmeans and the existing algorithms(N=50)

Figure 4, describes the runtime(ms) computation of the traditional models to the present model in dynamic WSNs. From the figure 4, it is observed that the present model has less runtime(ms) than the traditional models when the number of nodes is 50.

Table 2: Runtime(ms) computation of the proposed probabilistic kmeans and the existing algorithms

IterationNo	K-means	K-Means++	Fuzzy-CMeans	Trust-ProbabilisticKmeans
#1	2769.63	2367.14	2265.57	2069.6
#2	2781.01	2732.04	2367.29	2054.47
#3	3193.82	2621.33	2471.05	1943.09
#4	2984.81	2476.74	2505.75	2016.76
#5	3223.77	2605.38	2441.58	2048.46
#6	2984.24	2600.42	2157.27	2063.88
#7	2958.78	2849.25	2362.92	2046.54
#8	3067.68	2325.46	2469.37	2023.25
#9	3132.2	2521.91	2325.22	1923.5
#10	2933.94	2437.94	2287.31	2090.15
#11	3201.05	2751.2	2270.03	2046.77
#12	2849.71	2835.28	2222.76	2005.65
#13	2939.56	2755.82	2353.72	1924.63
#14	3062.54	2810.21	2272	2089.12
#15	2854.07	2564.18	2497.68	2017.39
#16	3113.19	2513.13	2332.79	2011.68
#17	3195.3	2333.03	2333.61	2028.65
#18	2811.41	2574.87	2196.83	1943.31
#19	2910.39	2747.94	2459.26	1990.96
#20	2903.94	2721.8	2372.16	2063.65

Table 2, describes the runtime(ms) computation of the traditional models to the present model in dynamic WSNs. From the table 2, it is observed that the present model has less runtime(ms) than the traditional models when the number of nodes is 75.

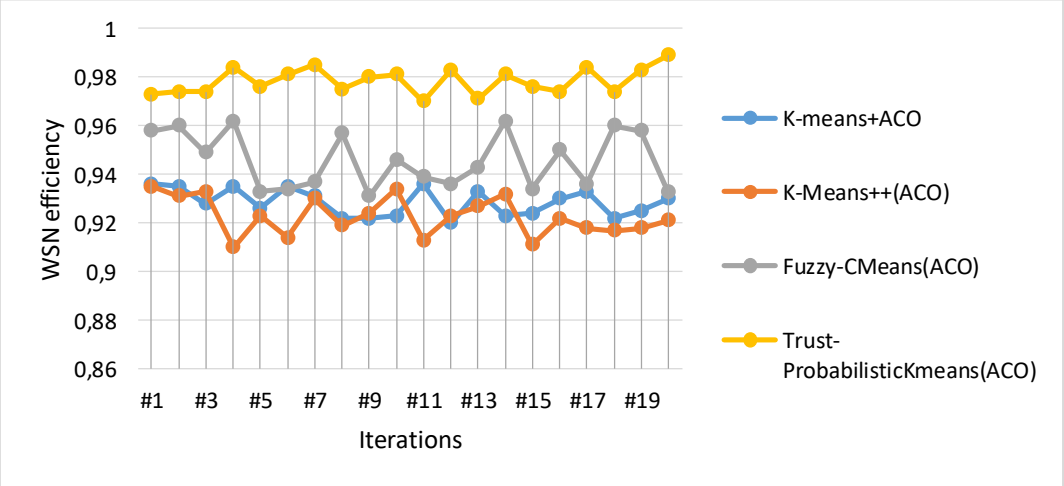

Figure 5: Comparative analysis of proposed trust-based efficiency to the traditional trust based cluster models on different iterations.

Figure 5, describes the WSN packet delivery efficiency of the traditional models to the present model in dynamic WSNs. From the figure 5, it is observed that the present model has better efficiency than the traditional models when the number of nodes is 75.

Figure 6: Sensor generated sample master key:

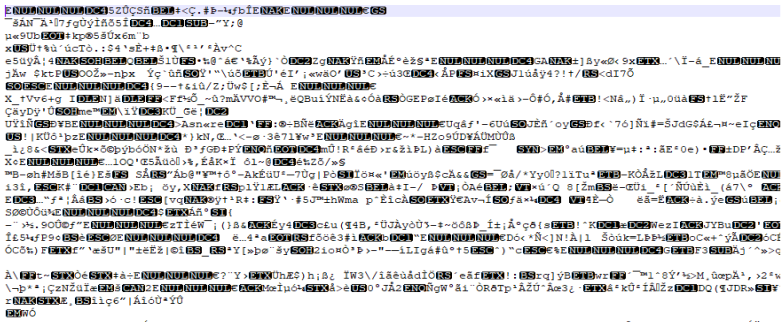

Figure 7: Sensor generated sample public key

Figure 8:Encrypted Sample Data:

€a6767874c74a5c9e591622a8a04445d4853e3ecae93136faa4c4f0bcc422f1179e41d049e2c5f
276109407f5b86ee64f1f5e9cc5aba4b1e9d884c3ef7e99e4ddE €˜• ÏØ«
ªlá´Rû¥ˆã¦_Q¥c-ºÂlòk• k†ºâÚ–Ÿl$>Ù`¸¯jç¢ý€e¡‰—+`ÖŒ• QB; —
‰Õê»»«ãßo3ôH®#)¬+Ú_T§òOä²hN

'i¶°™qkÝ:šØþYé ö×€□w›9ý1·ûA@E
€a6767874c74a5c9e591622a8a04445d4853e3ecae93136faa4c4f0bcc422f1179e41d049e2c5f
276109407f5b86ee64f1f5e9cc5aba4b1e9d884c3ef7e99e4dd[E
€bài6>,/6©au”oA¬HÈ*?x1œ'cî¥Ë¬¯

¾+B,`,ÜÙØ‰Üq¿…Ï^ÏSXivúAB_ZF□ŠO?F`8†c

¾ÄÉŒ~nÀd□˜ fÌßÉyg¤áÞ~ºÕê.ú§%qVâ~ù`jØH¥‘œð®‡
3E
€uÁ• å>*————————————————Ño.V%3ÄÝ4}c+Ûa□™íM]Žð‰v…D“´&TX¨
Y3• e?©Þròù]éIÚ–O`yþ¸• Xðô¥aÕìM"h2| ëëø□‘4¢•,ã2è,Fk^SÙ¶¿/¸ÓP•k"«^y´êÃ-D
Z$ûËœ(JÎÉÀdWuøù²w.Î½än'6Ó-G³¬½ýf¢mx²ðÏ™Z{+ÿœ„VM24—f!Žã“ «¼ñöùÉ□q|nõ¬Å4
• —”MÇå:• -

ôöEòã³><?UÊïÏï
ÝOÃlÞ-íøS• ë9
;hÅºœi$Aá|n ¦Î,,
†¤Î4Öp-µƒløm
QWþ¥

©uqJ’Žà«:úŸn!
!®Ã@Î¤ôuáØû
b• ³

Table 3: Comparative analysis of proposed model to traditional integrity algorithms on sensor data.

Model	Integrity Sensitivity	Integrity runtime(ms)
MD5	115	4353
SHA512	119	3975

whirpool	121	3684
NonLinear-integrity	131	3254
ProposedIntegrity	133	2974

Table 3, describes the comparison of the proposed optimized integrity algorithm sensitivity and runtime to the existing algorithms on large sensor data. From the table, it is noted that the present algorithm has high sensitivity and less runtime than the existing algorithms.

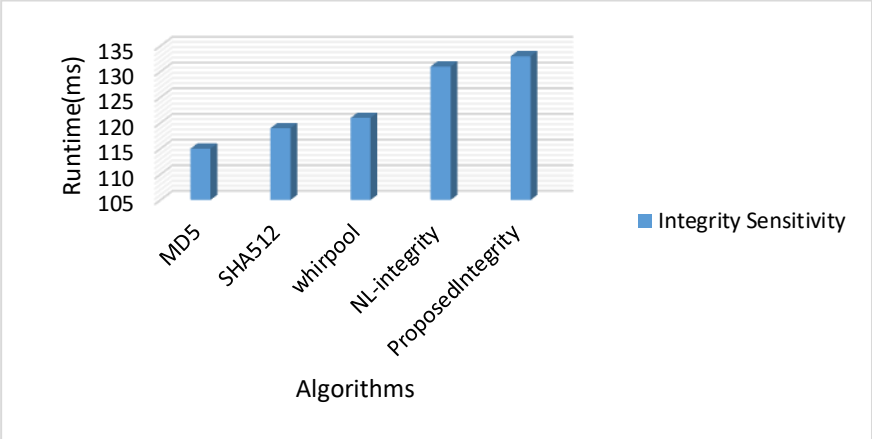

Figure 9: Comparative analysis of proposed model to traditional integrity algorithms on sensor data.

Figure 9,describes the comparison of the proposed optimized integrity algorithm sensitivity to the existing algorithms on large sensor data. From the figure, it is noted that the present algorithm has high sensitivity and less runtime than the existing algorithms.

Conclusion:

`In this paper, Wireless sensor networks (WSNs) dynamic topology structure established with two different network sizes and communication. Data privacy, node path planning and Data integrity are computed and tested with traditional methods. The proposed model resolved all the traditional methods issues and trust-based node integrity verification and privacy preserving model is implemented for dynamic WSNs. In this model, a hybrid ACO based node trust probability and path planning implemented with new local update and global update measures. The results proved that the present trust based model has better runtime, hash variation and privacy preserving metrics than the traditional WSNs cluster based authentication protocols.In future, apply the same model with mobility and calculate the energy model.

References:

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, .Wireless sensor networks:a survey.,Computer Networks 38 (4), 2002, 393.422.

[2] K. Romer, O. Kastin, and F. Mattern, "Middleware challenges for wireless sensornetworks," ACM SIGMOBILE Mobile Computing and Communications Review, Vol 6, No. 4, 2002, 59-61.

[3]R. Shorey, A. Ananda, and W. T. Ooi, "Mobile,wireless, and sensor networks," 1st edition, IEEE Press, John Wiley & Sons, 2006.Int. J. Advanced Networking andApplications, Volume: 02, Issue: 04, Pages: 745-754 (2011)

[4]J.K. Hart and K. Martinez, .Environmental Sensor Networks: A revolution in the earthSystemscience,. Earth-Science Reviews, 78., 2006, 177-191.

[5] T. Bokareva, W. Hu, S. Kanhere, B. Ristic, N.Gordon, T. Bessell, M. Rutten, and S. Jha,"Wirelesssensor networks for battlefield surveillance", 2006.[Online] Available:http://www.cse.unsw.edu.au/~tbokareva/papers/lwc.html

[6] E.J. Duarte-Melo and Liu Mingyan, "Analysis of energy consumption and lifetime ofHeterogeneouswireless sensor networks," Global Telecommunications Conference,2002.GLOBECOM '02. IEEE , vol.1, Nov. 2002, 17-21.
[7] K. Lu, Y. Qian and J. Hu, "A framework for distributed key management schemes inheterogeneous wireless sensor networks," Performance, Computing, andCommunications Conference, 2006. IPCCC 2006. 25th IEEE International, vol., no.,April 2006.
[8] Liyang Yu, Neng Wang, Wei Zhang and Chunlei Zheng, "Deploying a HeterogeneousWirelessSensor Network", International Conference on Wireless Communications,Networking and Mobile Computing, WiCom 2007, vol., no., 21-25 Sept.2007, 2588-2591.
[9]Padmalaya Nayak, Member, IEEE, and Anurag Devulapalli,A Fuzzy Logic-Based Clustering Algorithm for WSN to Extend the Network Lifetime, IEEE sensors journal, vol.16, no. 1, january 1, 2016
[10]M. Younis, M. Youssef and K. Arisha, .Energyaware management in cluster-basedsensor networks., Computer Networks 43 (5), 2003, 649-668.
[11] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, .Energy-efficientcommunication protocol for wireless microsensor networks,. In Proceedings of the 33rdAnnual Hawaii International Conference on System Sciences, 2000,no. 10, vol.2, Jan.2000, 4-7.
[12]S. Lindsey and C.S. Raghavendra, .PEGASIS:power efficient gathering in sensorInformationsystems,. in: Proceedings of the IEEE Aerospace Conference, BigSky,Montana, March 2002.
[13] Anand.Nayyar and Rajeshwar.Singh,"Ant Colony Optimization (ACO) based Routingprotocols for Wireless Sensor Networks (WSN): A Survey," International Journal ofAdvanced Computer Science and Applications., Vol. 8, No. 2, 2017.
[14] A. Manjeshwar and D.P. Agarwal, .APTEEN: a hybrid protocol for efficient routing andcomprehensive information retrieval in wireless sensor networks,. in: Parallel andDistributed Processing Symposium. Proceedings International,IPDPS 2002, 2002,195.202.
[15] K. Akkaya and M. Younis, .A survey on routingprotocols for wireless sensor networks.,Elsevier Journal of Ad Hoc Networks 3 (3), 2005, 325.349.
[16] M. Younis, M. Youssef and K. Arisha, .Energyawaremanagement in cluster-basedSensornetworks., Computer Networks, 43 (5), 2003, 649-668.

[17] Y.T. Hou, Y. Shi and H.D. Sherali, .On energyprovisioning and relay node placementfor wirelesssensor networks,. IEEE Transactions on WirelessCommunications 4 (5),2005, 2579.2590.
[18] K. Dasgupta, K. Kalpakis and P. Namjoshi, .Anefficient clustering. based heuristic forDatagathering and aggregation in sensor networks,. in:Proceedings of the IEEEWireless Communications and Networking Conference (WCNC, 2003), NewOrleans,LA, March 2003.
[19] E.P. de Freitas, T. Heimfarth and C.E. Pereira,.Evaluation of coordination strategies forheterogeneous sensor networks aiming atsurveillance applications,. in: Proceedings of IEEE Sensors (SENSORS), Christchurch, New-zealand,2009, 591.596
[20] J.M. Corchado, J. Bajo, D.I. Tapia and A. Abraham,.Using heterogeneous wirelesssensor networks in atelemonitoring system for healthcare,. IEEE Transactions onInformation Technology in Biomedicine 14 (2), 2010, 234.240.
[21]M. Yarvis, N. Kushalnagar and H. Singh,Exploiting heterogeneity in sensornetworks,.IEEE INFOCOM, 2005.
[22] A.A. Abbasi and M. Younis, "A survey onclustering algorithms for wireless sensornetworks"Computer Communications 30, 2007, 2826.2841.
[23] G. Gupta and M. Younis, .Load-balanced clusteringin wireless sensor networks,. in:Proceedings of the International Conference on Communication (ICC 2003),Anchorage, Alaska, May 2003.