IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. III (Nov – Dec. 2014), PP 37-49
www.iosrjournals.org

SSEGR: Secure Single-Copy Energy Efficient Geographical Routing Algorithm in Wireless Sensor Networks

Lata B T[1], Raghavendra M[1], Tejaswi V[2], Shaila K[1], Venugopal K R[1], S S Iyengar[3], L M Patnaik[4]

[1](Dept. of CSE, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, INDIA.)
[2](Dept. of CSE, NITK, Surathkal Bangalore, INDIA.)
[3](Director and Ryder Professor, Florida International University, USA.)
[4](Honorary Professor, Indian Institute of Science, Bangalore, India.)

Abstract: *Geographical Routing Technique is a new trend in Wireless Sensor Networks in which the sensor nodes are enabled using Global Positioning Systems (GPS). This helps to easily detect the position of their neighboring nodes. The power consumption is more in the existing routing algorithms, since the nodes build the routing tables and the neighboring node IDs are determined by searching the routing table. In this paper, we have proposed Secure Single-Copy Energy Efficient Geographical Routing (SSEGR) algorithm in which the data traffic and energy consumption is minimized using single copy data transfer. In SSEGR, initially one copy is transmitted to the next node using greedy approach and another copy is preserved in the sending station. If acknowledgment is not received even after timeout then the second copy is transmitted. This dynamic single copy scheme reduces the data traffic in Wireless Sensor Networks. Security algorithms are incorporated in every sensor node to prevent any malicious node attack that disturb the normal functioning of the network. Simulation result shows that the performance of the proposed algorithm is better interms of packet delivery probability and energy consumption in comparision with existing algorithms.*

Keywords: *Energy Efficient, Event Detection, Event Driven, Geographical Routing, Single Copy, Wireless Sensor Networks.*

I. Introduction

Event Driven Wireless Sensor Networks (EWSNs) are composed of large number of sensor nodes that are deployed in the terrain of interest to sense physical parameters such as temperature, pressure etc. The event is detected in a distributed manner and the final decision is delivered quickly to users in an energy efficient manner. A sensor node perform various tasks like sensing (Collects information about a determined phenomena), data forwarding/routing (transmits data to neighbor nodes) and performs computation. After successful sensing of data, it has to be delivered to the base station along with its location. The location is calculated using Global Positioning System.

EWSNs is based on the occurrence of an event at the nearby sensor nodes. The sensor nodes transmits the data collected to the base station, which is located at some corner of the deployment area. In traditional approach, the data transfer from sensor nodes to base station demands huge computation from intermediate nodes. The network has to handle large data flow in the network, so the data transfer takes place using multiple paths. There is a possibility of the same copy of the information being transferred in multiple paths, this reduces the battery power below threshold value. The network lifetime and energy consumption are two important factors that effects the performance of sensor networks. The energy consumption of the network can be minimized using chain network in the detection process. In the chain network, output of one sensor is fed as input to the next sensor. Chain networks are used to limit the throughput in each sensor-to-sensor link to save energy with low error probability at the sink. There are two types of errors that occur in these types of networks- (i) Miss Detection - When an event has occurred but the network does not detect it, (ii) False alarm - The network signals an alarm, even if the event has not occurred.

Various routing protocols have been developed. The routing protocols in sensor networks are categorized into two groups. They are: Pro-active (table-driven) routing, Reactive (on-demand) routing and Geographical routing. (i) Pro-active Routing Protocols: It maintain a fresh list of routes by periodically distributing routing tables throughout the network, but the reconstruction of the routes due to link failure is slow. (ii) Reactive Routing Protocols : It establishes a route on demand by flooding the network with route request packets, which consumes less energy. However, this type of routing (Reactive/on-demand) results in high latency time due to route finding process. (iii) Geographic Routing : It is a routing principle that depends on geographic position information and is used extensively in wireless networks.

The functions used for detection and transferring of sensed data efficiently to the base station are: Local Event Detection : When an event like fire occurs, gradually the smoke, temperature, pressure etc., starts increasing in that particular area. The sensor nodes present in the affected area gathers the statistics of the information, processes these details and decides whether the parameters are increased to an extent which causes fire. When the occurrence of an event is confirmed by all the nodes in the area, then the decision is transferred to the base station; thus, avoiding unnecessary information transmission to the base station which consumes more energy and in turn decreases the network lifetime. Base station takes remedial action only for the true confirmed events.

Global Data Transfer : The reliable transfer of information to the base station after successful detection of true events is referred to as the Global data transfer. This can be achieved by using timers and acknowledgment signals. Also, the lifetime of the packet must be considered to avoid obsolete information reaching the base station. So, obsolete data must be deleted and the sensors must retransmit whenever timeout occurs.

Multipath Routing : Most of the multipath routing schemes are table based algorithms. In these algorithms same data is transmitted in different routes so that at least data in one of the route will successfully reach the base station. Creating and maintaining the neighbor list is a tedious task in battery operated WSNs. In this approach, nodes communicate frequently to update the information about their neighbors. Then, the entire data is forwarded to the base station, where the actual event detection and remedy is decided.

Traffic Reduction : In order to successfully transmit data to the base station, with reliability, local and global algorithms are developed that rely on timeout and acknowledgments. The alarm is generated only when the event is detected by majority of the neighboring nodes. Then, the action taken by the base station will be correct because only correct alarm packet has reached the base station. obsolete packets will be filtered out at intermediate nodes. This eliminates false alarm packets thus reducing network traffic.

Geographical Routing: Geographic Routing also called Geo-routing or Position-based Routing. It is a routing principle that relies on geographic position information used mainly in wireless networks. In geographic routing the destination address is used instead of network address. The position information routing is used for the packet radio networks and interconnection networks. Geographic routing requires that each node determine its own location and that the source is aware of the location of the destination. With this information, a message can be routed to the destination without knowledge of the network topology or a prior route discovery.

There are various approaches, such as single-path, multi-path and flooding-based strategies. Most single-path strategies rely on two techniques: greedy forwarding and face routing. Greedy forwarding tries to bring the message closer to the destination in each step using only local information. Thus, each node forwards the message to the neighbor that is most suitable from a local point of view. The most suitable neighbor can be the one which minimizes the distance to the destination in each step (Greedy). In Greedy routing, a node makes its routing decision by Standard Euclidean Distance calculation based on the set of local coordinates. Traditional greedy routing algorithm fails due to the problem of local minimum. In the compass routing, the minimum angle between the neighbor and destination is selected. But greedy forwarding leads to a dead end from which position the packet cannot be forwarded further. The recovery from this state is possible using Face Routing techniques.

Routing protocol uses GPS(Global positioning system) to find the location information. These geographic forwarding does not require routing tables maintenance and routing construction prior to or during the forwarding process. In this paper, an efficient event detection mechanism is used, in which cluster center decides the occurrence of event after several rounds of local data exchange with the neighboring nodes. If the cluster head is satisfied about the occurrence of an event, then the gathered data are forwarded to the base station.

Motivation: Many routing algorithms developed for WSNs do not consider the limited resource constraints of the sensor nodes. The work by Lulu[12] uses dynamic multicopy scheme to ensure reliable data transmission to the base station. The algorithm provides good reliability of the alarm packet delivery, but consumes huge energy. Transmission of multiple copies of the data results in data redundancy.

Contribution: In this paper, the events are detected and transmitted in real time. The event characteristics are analyzed and raw data is processed during implementation. Secure Single copy Energy Efficient Geographical Routing (SSEGR) algorithm proposed in this paper, improves the network lifetime. Geographic routing is applied to route data from sensor nodes to the base station. Each intermediate node selects the next forwarding node based on GPS information. Energy consumption is minimized by limiting the number of routes towards the base station by adopting single copy scheme. The delivery probability is increased and the event reaches the base station quickly and reliably. SSEGR algorithm can be applied to a continuous surveillance WSNs with heterogeneous sensing fidelity requirements over different event areas.

Organization: The rest of the paper is organized as follows: Section II gives a brief review of Related Works and the background of the work is discussed in Section III. Section IV contains the problem definition

while the network model is described in Section V. Mathematical model is developed in Section VI and the algorithm is presented in Section VII. Section VIII discusses the simulation and performance result evaluation of the algorithm and Conclusions are presented in Section IX.

II. Related Work

Xiaonan et al., [1] proposed a scheme for constructing an Internet Protocol (IP) over low-power wireless personal area networks. It includes cluster generation, cluster-tree construction, and cluster-tree repair algorithms. This minimizes the total number of nodes included in a cluster tree thus reducing the routing cost. When a cluster head or a cluster associate node fails or moves, a new cluster head or cluster associate node is elected to maintain the cluster-tree topology in a cluster tree repair algorithm. The stability of cluster-tree decreases with the increase in the movement of the nodes.

Matteo and Marco [2] present a wireless sensor network configuration for fire detection applications. A chain network is considered for GP (all nodes observe same event) and LP (subset of nodes observe the event) phenomenon, to reduce the transmissions and then minimize power consumptions by making a local binary decision; each node makes a local decision, about target absent/present considering its own observation and also the decision made by the previous node. Fusion rules are used to minimize the throughput per link and error probability at the sink. They proposed and analyzed a one-node memory decision rule with a throughput of less than two bits per link, if all of them observe the same event. The decision is based on local and previous node observation, wrong decision may be forwarded.

Phani et al., [3] proposed a framework for distributed event detection in WSNs. Collaboration is considered for event detection when there are failures and low energy of nodes. The framework consists of two protocols that build a tree by using a communication model. This framework is a part of Component Oriented Middleware for Sensor networks (COMiS). In COMiS framework, components are loaded as and when required based on the application semantics. It does not support mobility of sensor nodes and priority of events in composite event detection.

Brad et al., [4] presented a Greedy Perimeter Stateless Routing (GPSR) for 2-D volumes in wireless datagram networks that uses the position of routers and packets destination to take decisions about packet forwarding. GPSR makes greedy forwarding decisions using immediate neighbors in the network topology, in which it uses local topology information to determine new routes correctly and quickly. In GPSR, the nodes forward the packet as far as possible. When a packet reaches a region, where greedy forwarding is impossible, the algorithm recovers by routing around the perimeter of the region.

SPEED [5] is a Stateless, end-to-end, real-time communication protocol for sensor networks. It provides three types of real-time communication services, namely, real-time unicast, real-time area-multicast and real-time area-anycast with minimal control overhead. SPEED satisfies stateless architecture, soft real-time, minimum MAC layer support, QoS routing and congestion management, traffic load balancing, localized behavior and void avoidance. It handles congested areas and guarantees data delivery if there is a greedy route between the source and destination. SPEED protocol has been tested only for ad-hoc sensor networks.

ESRT (Event-to-Sink Reliable Transport) [6] protocol addresses the transport problem in Wireless Sensor Networks (WSNs) to achieve reliable event detection with minimum energy expenditure. It includes a congestion control component that serves the dual purpose of achieving reliability and conserving energy. This self-configuring nature of ESRT helps to adapt dynamic topology and random deployment and to conserve scarce energy resources. It mainly runs on the sink and require minimal functionality at resource constrained sensor nodes. The metrics addressed in this work are congestion and energy while concurrent events in the sensor field are not considered.

Kang et al., [7] proposed an approach for robust Geographic Routing (GR). It uses rate control, packet scheduling and trust-based multi-path routing. The GR is a greedy routing algorithm based on geography in which only nodes maintain location information of their one hop neighbors. Routing decision is either made locally or dynamically. The implications of range-free/multi-hop localization algorithms in terms of secure localization or location verification have not been considered in this protocol.

Thrasyvoulos et al., [8], [9] proposed a number of different single-copy routing strategies, such as Direct Transmission, Randomized Routing Algorithm, Utility-based Routing and Seek and Focus Routing Protocol (A Hybrid Approach). The metrics used in the comparison are the average message delivery delay and the number of transmissions per message delivered. These routing algorithms do not justify the cost incurred by a single transmission, while making a forwarding decision.

Chris et al., [10] proposed threat models and security goals for secure routing in wireless sensor networks. They have introduced two novel classes attacks against sensor networks; i.e. sinkhole attacks and HELLO floods. They have presented the detailed security analysis of all the major routing protocols and energy conserving topology maintenance algorithms for sensor networks. Bo et al., [11] introduced a lightweight security scheme for detecting selective forwarding attacks. The detection scheme uses a multi-hop

acknowledgement technique to launch alarms by obtaining responses from intermediate nodes. Communication overhead increases in multi-hop acknowledgement scheme. If the number of packet drop increases, communication overhead also increases as more alarm packets are generated and forwarded.

Lulu et al., [12] introduced an Efficient Event Detecting Protocol (EEDP) specified for event monitoring applications. In the event occurring area, each node broadcasts its primary detection result to make a decision corporately and then the decision-made node will choose the next hop using the underlying routing protocol to forward a single alarm packet. To improve the reliable transmission of the single alarm packet, A dynamic multi-copy scheme is used. Multi-copy scheme is used here which consumes large amount of energy when compared with single copy schemes. Sleep-wake scheduling scheme can be used to conserve energy.

Reza et al., [13] proposed a BSMR(Byzantine-Resilient Secure Multi-cast Routing), on-demand multi-cast protocol for multi-hop wireless networks that provides resiliency against a representative set of strong Byzantine attacks (black hole, wormhole, and flood rushing). BSMR also prevents attacks that try to prevent or arbitrarily influence route establishment. BSMR mitigates the attacks, while incurring a small communication overhead. Quek et al., [14] investigated the problem of binary decentralized detection in a dense and randomly deployed wireless sensor network (WSN), whereby the communication channels between the nodes and the fusion center are bandwidth-constrained. A consensus flooding protocol is compared with parallel fusion architecture (PFA) and cooperative fusion architecture (CFA), where, the degree of cooperation among the sensor nodes varies and each node is restricted to sending a 1-bit information to the fusion center. Expressions are derived for the probability of decision error at the fusion center and the average energy consumption for each architecture is analyzed. This work can be extended to to a distributed multi-target classification problem of WSNs.

Feilong et al., [15] proposed a scalable architecture for Wireless Mesh Sensor Networks (WMSNs) and introduced a secure routing protocol (SecMLR). In WMSNs, multiple gateways are used to reduce the average transmission hops. However, the sensor nodes around gateways still consume more energy to forward packets to other nodes. Roy et al., [16] introduced a novel lightweight verification algorithm by which the base station can determine if the computed aggregate (predicate Count or Sum) includes any false contribution. The protocol is limited to ring based topology.

Nicholas et al., [17] designed DRAGON, an event detection and tracking protocol which is able to handle all types of events including region events with dynamic identities. It employs two physics metaphors: event center of mass, to give an approximate location to the event; and node momentum, to keep track of event splits and merges. It is energy efficient and scales well with problem size and complexity. It's execution time and costs scale linearly with the number of events and grow better with respect to event coverage.

Virtual Energy-Based Encryption and Keying (VEBEK) [18] scheme for WSNs significantly reduces the number of transmissions needed for re-keying to avoid stale keys. VEBEK is a secure communication framework where sensed data is encoded using RC4 encryption mechanism. It does not exchange control messages for key renewals; uses one key per message and is therefore able to save more energy and is less chatty. It is able to efficiently detect and filter false data injected into the network by malicious outsiders. This work does not address insider threats and dynamic paths.

Ren et al., [19] designed an Energy-Balanced Routing Protocol (EBRP) by constructing a mixed virtual potential field in terms of depth, energy density, and residual energy. It forces the packets to move toward the sink through the dense energy area so as to protect the nodes with relatively low residual energy. EBRP finds efficient routes for each data source to the sink and saves energy by eliminating the loops. It belongs to the class of data-gathering based routing algorithm, and does not deal with data dissemination, point-to-point communication and routing loops.

Kui et al., [20] presented Secure and fault-tolerant Event Boundary Detection (SEBD) scheme. It greatly mitigates the security threats caused by compromised nodes, cheating attacks, impersonating and colluding attacks, replay attacks, node relocation and replication Attacks. The computation costs incurred by the security related operations in SEBD is light-weight. It performs very well, when node compromise probability equals to zero and very good at detecting boundary nodes. Communication overhead increases with increasing range of neighbors.

Jing et al., [21] introduced a novel spatiotemporal approach to ensure secure range queries in event-driven two-tier sensor networks with low communication overhead. It achieves high query efficiency by preventing compromised master nodes from reading hosted data. It allows the network owner to verify the authenticity and completeness of any query result. The bucketing technique is used, which partitions the queriable attribute domain into g >= 1 consecutive non-overlapping regions (buckets), sequentially numbered from 1 to g. As the g increases, the detection probability of Hybrid-based Spatial Crosscheck (HSC) slightly decreases and communication costs increase.

Lee et al., [22] proposed a hybrid data-gathering protocol that dynamically switches between the event-driven data-reporting and time-driven data-reporting schemes. Two algorithm i.e., parameter-based event detection (PED) algorithm and parameter-based area detection (PAD) algorithm are presented. In PED, threshold value is used to determine the occurrence of an event. The novel aspect of this approach is that sensor nodes that seem to detect an event of interest in the near future, as well as those nodes detecting the event, become engaged in the time-driven data-reporting process. Since, the behaviors of the hybrid data-gathering protocol depend on the configurable parameters, this work can be extended to develop algorithms for the dynamic selection of configurable parameters based on the characteristics of the target environment.

Wang et al., [23] designed a simple localized routing algorithm, called Localized Energy-Aware Restricted Neighborhood routing (LEARN). It guarantees the energy efficiency of its route and can be extended into three-dimensional (3D) networks and for mobile networks.

Zhang et al., [24] proposed a novel online routing scheme, called Energy-efficient Beaconless Geographic Routing (EBGR). It provides loop-free, fully stateless, energy-efficient sensor-to-sink routing at a low communication overhead without the help of prior neighborhood knowledge. It is based on geographic routing and power-aware routing. The expected total energy consumption along a route towards the sink under EBGR approaches to the lower bound with the increase of node deployment density. There is unbalanced energy consumption in the network.

III. Background Work

The Lulu et al., [25] adopts geographical routing to satisfy the time critical requirement for EEDP which is designed for event monitoring applications. Global Positioning System (GPS) [26] relies on geographic position information and is used to find the location information that is required for in routing protocol. Using GPS, the source sends a message about the geographic location of the destination. These geographic forwarding does not require routing tables maintenance and routing construction prior to or during the forwarding process and dissemination of topology information.

Geographic routing offers low overhead and low latency solution which is very important for delay sensitive applications such as event monitoring. The information is captured by the sensor nodes in the event occurring area and each node broadcasts its primary detected result to make a decision cooperatively. The advantages of this protocol are: (i) Decision are locally made in the event area and only specific results about the event is sent to the sink and (ii) Dynamic multi-copy scheme used to ensure the reliability of the alarm packet delivery.

EEDP consist of two procedures : (i) Primary Detection Procedure(PDP) and (ii) Emergency Routing Procedure(ERP). PDP detects a composite event. Observations made by sensors x^i_m is the observation of m^{th} sensor of node i. The algorithm for taking the decision consists of two types of decision rules : (a) Single Decision Rule(SDR) and (b) Composite Decision Rule(CDR). Threshold of node i for the m^{th} atomic event and the combination output of SDR is considered in decision making.

The SDR is used for the primary atomic decision of each sensor node, while CDR is used for further accurate decision combining with the detection results of all the atomic events. Each node i in Emergency Source Nodes (ESNs), conducts a local primary decision message. The local primary detection message broadcasted to its neighbors, to make further decision cooperatively. In the broadcast process, timer, ack and timeout mechanism is used to ensure reliability. The algorithm uses local broadcast and global broadcast strategies.

During this process two types of nodes are used: (i) ESN - Emergency Source Nodes-These are sources of events. and (ii) EFN - Emergency Forwarding Nodes-These nodes does not have enough data to send but forwards all incoming packets to next node in the direction of base station. Each node uses SDR to make primary decision if the sensed data exceeds a predefined analog value. Emergency routing procedure uses end-to-end delivery. Each node uses greedy forwarding strategy relaying the packet to a neighbor, closer to the destination area. The event node continues to send the alarm packet to destination periodically until it receives an acknowledgment from destination. This ensures 100% data delivery.

IV. Problem Definition

In WSNs, the data packets can take a single path for transmission or copy of the data can be transmitted in multiple paths as discussed in [12]. When multiple copies of the data packets are transmitted, there is a possibility of the adversary having a copy of the data by compromising with the node and even resulting in the energy consumption. Energy consumption can be minimized by sending only a single copy of the data using geographical routing techniques. The node compromise attack can be avoided by selecting the nodes randomly. The objectives of the work are to:

- Guarantee delivery probability and minimize energy consumption by developing energy efficient geographical routing technique.

- Overcome node compromise attack.

V. Network Model

The system model proposed is a static, homogeneous network that works on Collaborate, Collate and Compare (CCC) formula. The data is collaborated in the source station and is collated to the next node. When acknowledgment is received, it is compared for modification if any, due to attack. Figure 1 shows the nodes A, B, C, D are neighboring nodes and the cluster is formed with node A as cluster head, while the nodes B, C, D are the cluster members. The sensed parameters are exchanged between these neighboring nodes and a final decision is arrived with respect to event. So, that only true event detection information is transmitted to the base station and eliminates false event. The data is encrypted by implementing the security algorithm in each node. The algorithm uses single copy instead of multiple copies, thus introducing security so that the events are correctly reported to the base station. The next hop selection is performed based on greedy approach, so that the time and energy required for searching a suitable node is minimized thereby increasing the network lifetime.

Table I

Table of Notations Symbol Definition

S_m (t)	Nodes carrying message
m	message
t	Time
Th(temp)	Threshold value of temperature
Th(pres)	Threshold value of pressure
Th(smoke)	Threshold value of smoke
M	Node lying outside the threshold boundary
H_n	Next Hop
tg	Global Timer
E(tx)	Energy
E(rx)	energy consumed during reception
E(sp)	Energy consumed during sleep state
b	Number of bits transmitted.
d	Distance between sender and receiver node
spc	Speed of transmissions
succ	Packets successfully reaching base station
gener	Packets generated at sensor nodes
del(p)	Packet deliver probability.
dr(p)	Packet drop probability
gps	Global Positioning System
cmp	Compare
th_d	Threshold distance
d_nn	distance of next node
nd_b	node distance from base station
db	Distance between base station

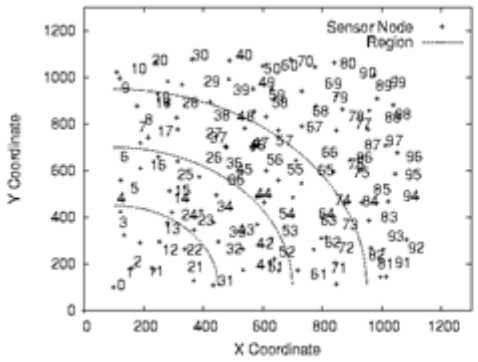

Fig. 2: Node Collaboration

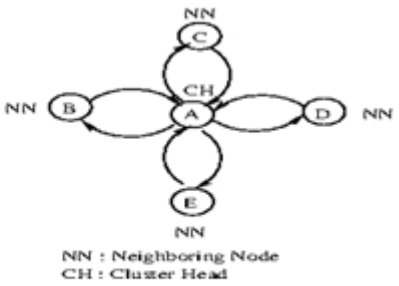

Fig. 1: Deployment of Sensor Nodes

Assumptions

(i) The base station is within the network region, located at the co-ordinates (0, 0).
(ii) The base station energy is infinite and is powered by ac mains power supply.
(iii) The nodes are stationary and each node is labeled with an unique ID.
(iv) The nodes are capable of adjusting power based on the communication distance.
(v) Links between nodes are reliable and has full duplex connectivity.

VI. Mathematical Model

A. Single Copy Strategy

The notations used in the model are explained in Table II. Let S_m (t) denote set of nodes carrying message m at time t. All the nodes follow single copy forwarding strategy i.e., there is at most only one copy of data moving in the path leading towards base station such that,

$S_m(t) \leq 1, \quad \forall t, m$ (1)

where, t is time and m is message.

B. Data Collection

Let Th(temp), Th(pres) and Th(smoke) are functional values of threshold. If the value exceeds threshold value, the particular event is triggered. Also Av(temp) is the average temperature and Ni is the i^{th} node in the deployment.

Av(Temp) = (N1(temp) + N2(temp) + ...+ Nr(temp)) / r (2)

Similarly, average of pressure and smoke are calculated by the cluster head.

Av(pres) = (N1(pres) + N2(pres) + ...+ Nr(pres)) / r (3)

Av(smk) = (N1(smk) + N2(smk) + ...+ Nr(smk)) / r (4)

In any case, if the values exceed the threshold value, then we can say that an event has occurred.

When,

Av(temp) $\geq$ Th(temp)
Av(pres) $\geq$ Th(pres)
Av(smoke) $\geq$ Th(smoke)

is satisfied then, the event is said to be triggered and an alarm packet is sent to the base station.

C. Local Broadcast and Next hop Selection

Let N = { n_0, n1, . . . , n_m} be a set of nodes present in the current region. Let M = {n_0,n_1,.....,n_k}
be the nodes which lie outside threshold boundary. Also, $|N|\ge|M|$. Next, the event is sent to any one of the nodes in set M.

In the next hop: H_n = threshold $\leq$ $node_i$ $\leq$ radio range (5)

Select node i such that its value lies between threshold and radio range.

A. Global Broadcast

Let t_g = global timer, d_1, d_2, . . . , d_n be the data packets and ACK be the acknowledgment packet then if

BS =
- $d_i \forall i | t \leq t_g$
  Base station sends ACK
- otherwise $\forall$ i|t $\geq t_g$
  Retransmit di

B. Total Energy Consumption

The total energy consumed is obtained using the formula given in [26]:

$$E_{tot} = E_{tx} P_{tx} + E_{rx} P_{rx} + E_{sp} P_{sp} \quad (6)$$

where, E_{tx}, E_{rx}, E_{sp} are energy consumed per second (Watt Hour) for transmission, receiving and sleep states. P_{tx}, P_{rx}, P_{sp} are percentage of transmission, reception and sleep over the total radio lifetime respectively.

F. Energy Consumption and Time Analysis

(i) Sending Energy

$$E_{tx}(b, d) = bE_{elec} + b \epsilon d^2 \quad (7)$$

E_{elec} is the energy consumed in transmitting b bits of data and d is the distance between sender and receiver.

(ii) Receiver Energy

$$E_{rx}(b) = bE_{elec} \quad (8)$$

(iii) Transmission Time

$$Tm_{tx}(b) = b / spc \quad (9)$$

where, b is the number of bits transmitted and the speed of data transmission is spc = 10^7 bits/sec

(iv) Propagation Time

$$Tm_{pr}(d) = b / spl \quad (10)$$

where, d is the distance between sender and receiver and the speed of data propagation transmission is spl = $2*10^8$ m/sec. The packet delivery probability del(p) is given by,

$$del(p) = succ / gener \quad (11)$$

where, succ = packets successfully reaching the base station and gener = packets generated at sensor nodes.

The Loss Rate LR is,

$$LR = 1 - del(p) \quad (12)$$

The packet drop probability dr(p) is,

$$dr(p) = 1 - del(p) \quad (13)$$

$$= (gener - succ) / gener \quad (14)$$

Let CE = consumed energy, IE = initial energy of sensor node, FE = final energy of sensor node, then consumed energy is,

$$\% CE = (IE - FE) / (IE) * 100\%$$

VII. SSEGR Algorithms

In Phase 1, the nodes are deployed along with the keys and each of the node is assigned with x and y coordinate values using GPS. In Phase 2, the data collection phase, the data relating to temperature, pressure, smoke is collected and is sampled at regular time intervals. This information is exchanged with the neighboring nodes. If the data average is above threshold value, then alarm is generated and the data transmission starts. Local broadcast algorithm transfers packets from node to node.

In Phase 3, Local and Global broadcast algorithm, timer is started after the alarm packet is sent. The Global Data transfer algorithm ensures end-to-end delivery. If the data packet has reached the base station then the global ack is sent. By chance, if global acknowledgment is not received within timeout then, only duplicate packet is retransmitted. During this process, care must be taken regarding packet lifetime and data stale, otherwise if any new packet is generated then, that is forwarded. Local broadcast uses greedy technique to take the data to the destination. Local broadcast algorithm ensures reliable transmission between nodes since it adopts local acknowledgment and timeout technique. If some other node is using it, then the transmission is delayed using Binary Exponential Back-off algorithm and ack, is transmitted using private key. If ack is not received within timeout, second copy is transmitted to the farthest node among neighbors, except the previous transmitted node.

Security attacks can occur at any time in the network due to misbehavior of the compromised nodes, deployed by the attackers. When the packet is received by these nodes, these nodes may not forward the packets further. When there are no compromised nodes, the packet reaches the base station. In this case the base station sends ack to the sender informing that the packet has reached successfully the base station. But in reality, packets are stopped by the compromised node. Thus, the message reaching the base station is prevented and the attacker successfully achieves his goal. This problem can be overcome by using security algorithms. The receiver of the acknowledgment checks security credentials and determines its integrity. If it is compromised, the path of the message is diverted, so that the compromised node is avoided. Suppose, if the acknowledgment is not generated by the compromised node or it has not reached the base station, the sender waits until timeout and then it retransmits the packets.

SSEGR Algorithms

```
Inputs: {int n, i, x, th, d, nd_b, d_b; measure at all nodes; t = gettemp( ); p = getpres( ); s = getsmoke( );}
Input: {Single Copy using Geographical Routing}
First Phase : Node deployment with keys:
For(i = 1 to n}{node[id] = i; node[x, y]=gps(x, y);  node[i].pk=key\_gen(  );}
Second Phase : Data Collection( )
X: Exchange information with neighboring nodes.
for(i=1; i<= nl.length; i++ ) { send alarm packet to base station if data collected is more than threshold  otherwise go to X. }
Third Phase : Global Broadcast( )
start_time=tg; local broadcast(  ); gto=check global timeout(  );
if (gto==1 and global_ack==1) then retransmit.
send(event, id);
if (id==base) then return global_ack;
y: search for next hop
for (i=1; I < = nl.length; i++)
{ if (thd < = dn n < = range ) then {
    If (ndb < nl[i].db) && (nl[i].cmp == 0) ) {k = check_media( );}
              If ( k == busy)} {delay(  ); goto  y;}
            Else {data = encry(data, key); recv(event, i, data);}
  recv(event, i,  data) {data = decr(data,key)  }; }
// When  Noise Collision occurs  in  medium
If ((data == malc(  ) ){return "error"; data = encr(event,  i, data); send(event, id);}
delay(  )  {d=d*2; wait(d)  }; }
```

VIII. Implementation

The nodes are deployed randomly in a 1000 m x 1000 m region as shown in Figure 1. The base station is placed at bottom left corner in the deployment area because there is a possibility of an event occurring in the deployment area and the sensor nodes may be affected. But if the base station is outside the danger area then, even if a fault is developed at the base station it can be easily detected. The complete area is divided into four regions. Region-I is near base station and Region-IV is near the border. Regions II and III are the intermediate regions. Nodes 7 and 24 are critical nodes in Figure 1. Due to greedy nature of data transmission, Critical nodes are shifted to Region II and Region III during deployment and hence the distribution of energy is indeterministic.

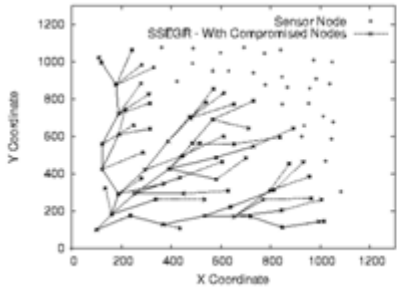

Fig. 3: Discovery of Routes from the Senors to the Base Station.

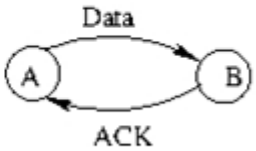

Fig. 4: Successful Data Transmission.

Data is routed from the sensor node to base station as shown in Figure 3. Keys are generated from the global key pool and they are assigned to the nodes before deployment. The data is encrypted before transmission to maintain data confidentiality. The sensors deployed in the event area will move the data path towards the base station. When the data moves towards the base station, the paths converges. Suppose a fault is detected in a particular path, immediately the intermediate sender changes the course of direction. Since the algorithm uses greedy strategy, the node throws the packet as far as possible to a non-faulty node. The packet reaches the base station with minimum effort, since it is not necessary for searching the neighboring list. The activities that occur during data transmission is explained below:

Case (i) : Figure 4 depicts successful data transmission to the next node. In this case, sending node A receives acknowledgment packet from receiver B before timeout.

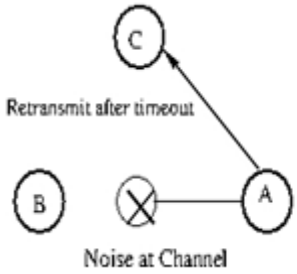

Fig. 5: Noise in the Ch

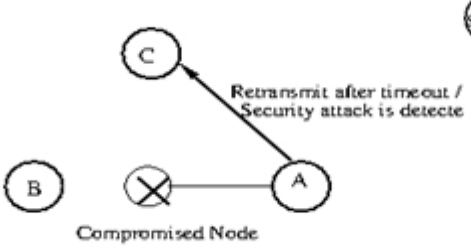

Fig. 6: Compromised Node.

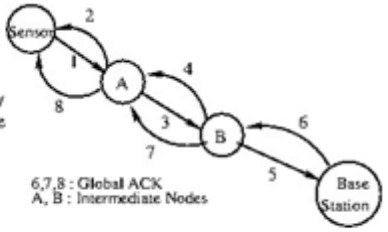

Fig. 7: Data Transmission towards Base station.

Case (ii) : The acknowledgment is not returned to the sender within timeout when the packet is lost as shown in Figure 5. The packet lost may be due to channel noise, noise in the signal or collision of packets, so the data packets are retransmitted.

Case (iii) : In the presence of compromised nodes as shown in Figure 6, then node A selects another node C to forward the packet. Thus, the packet traverses in a new path avoiding the attacker.

The complete processes of data transmission from source node where the event is generated and its flow to the base station is shown in Figure 7. Data transmission is done in two phases. In the first phase, reliable local transmission is guaranteed by using timeout and acknowledgment mechanisms. At the beginning of the task, the local timer is started. When a correct acknowledgment is received, the task is completed. In the second phase, sensor to base station data transmission known as global data transmission is determined by summing the local transmissions. The timer is started at the beginning of data transmission and if acknowledgment is not received within the timeout period then duplicate of the previous data is transmitted. The path diversion takes place when:

- The received acknowledgement is found to be compromised.
- Acknowledgement is not received even after time-out.
- the original packet or acknowledgement is lost due to noise and after timeout, retransmission takes place.

IX. Simulation and Performance Analysis

A. Simulation Setup

The proposed, Secure Single-copy Energy Efficient Geographical Routing algorithm is implemented using NS-3 simulator [27] in Fedora10. The Waf [28] and Waf [29] is a python-based build tool. Simulation parameter are depicted in Table III. The area of node deployment is considered to be 1000m x 1000m with the base station placed at origin (100, 100) as shown in Figure 1, the nodes are deployed randomly and the transmission range is set to 300m. The algorithm is evaluated for 100 to 150 nodes with 1000 seconds of simulation runs. The network security is verified by varying the number of malicious nodes in each simulation run.

B. Performance Evaluation

Simulation results mainly concentrates on residual energy and determination of the delivery probability. All the malicious nodes are accurately detected and significant improvement is achieved in successful packet delivery ratio. The energy remaining at the end of simulation by varying the number of compromised nodes is shown in Figure 8. The residual energy in the sensor nodes on an average varies between 494.7W to 494.9W with the existence of compromised nodes.

Comparison of the energy consumed with increase in the number of nodes is shown in Figure 10. The graph shows the residual energy at the end of the simulation after 10 seconds considering only the first 100 nodes. The energy consumed is more in EEDP when compared to SSEGR as EEDP transmits multiple copies of the same data. In SSEGR, only one copy of the data is transmitted and data redundancy is almost nil in the network. The energy consumed by SSEGR without any compromised nodes i.e., considering an ideal condition the energy consumed is reduced by almost 2% in comparison with EEDP. When compromised nodes exists, then the energy consumed is reduced by 1% compared with EEDP as some amount of energy is utilized to detect the attacks and divert the path. It is observed in Figure 10, that overall residual energy of SSEGR, with compromised nodes, it is between 494.9 Watts to 494.4 Watts, where as for EEDP, it is between 493.8 Watts to 493.5 Watts. Data is delivered securely avoiding the multiple copies of same data transmission in our protocol.

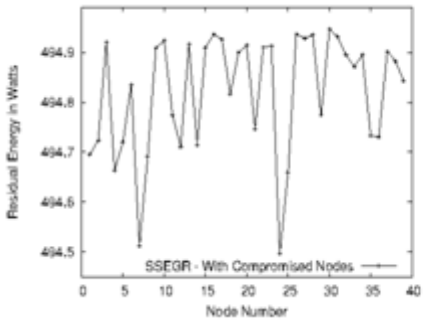

Fig. 8: Variation of Residual Energy using SSEGR with Variation in Compromised Nodes

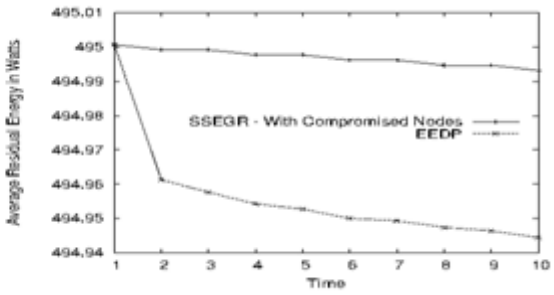

Fig. 9: Utilization of Energy with increase in Time.

The energy utilized per second is shown in Figure 9. First, the sum of the remaining energy of all the nodes (except base station) is calculated and their average is determined. The energy consumed by SSEGR algorithm is less compared to EEDP. The energy consumed decreases rapidly as the time progresses whereas it is uniform in the case of SSEGR. Average residual energy of SSEGR is 0.0081% more than the EEDP. At the base station, line power supply is not so important compared with the battery power of sensor nodes. Hence, the remaining energy of node 0 is not shown in the Figure 9.

The delivery probability is analyzed with respect to loss rate in Figure 11 that clearly shows, delivery probability decreases with the increase in losses i.e., Less number of packets are delivered to the base station. Delivery Probability with respect to loss rate is almost 70% better than previous work. When the loss rate is between 0 to 0.2, data loss is less, less number of nodes are compromised and delivery probability is high. As the compromised nodes increases, data loss also increases respectively, which is observed in Figure 11. As the data loss rate changes from 0.2 to 1, delivery probability decreases rapidly in EEDP in comparison with SSEGR. From simulation results, the delivery probability is between 0.2 and 1.0 for EEDP as shown in Figure 12. The delivery probability for our algorithm varies between 0.3 and 1.0 for SSEGR-compromised node. The input is stopped at the 10th second of the simulation. If a packet's TTL exceeds its value then that packet is discarded in the intermediate nodes or routers. Delivery Probability is 50% better than previous work. Input is stopped at the 10th second, delivery probability is constant up to 10th second.

Hop-count versus number of packets delivered is calculated and plotted in Figure 13. The simulation is run for a range of 300 meters. Packets delivery rate is higher in SSEGR algorithm. The hop count from sensor to base station varies between 1 and 5. If the event occurs is very near to the base station then it is at 1 hop distance, while it is 5 hops if the event occurs at border of the area. The number of packets delivered in one hop is 87.5% more than previous work. When the hop count and number of compromised nodes increases, the number of packets delivered is more in SSEGR in comparison with EEDP. When nodes are not compromised, even if the hop count increases, the number of packets delivered is more in SSEGR comparison with EEDP, since packets are routed securely and multiple copies of the same data is avoided.

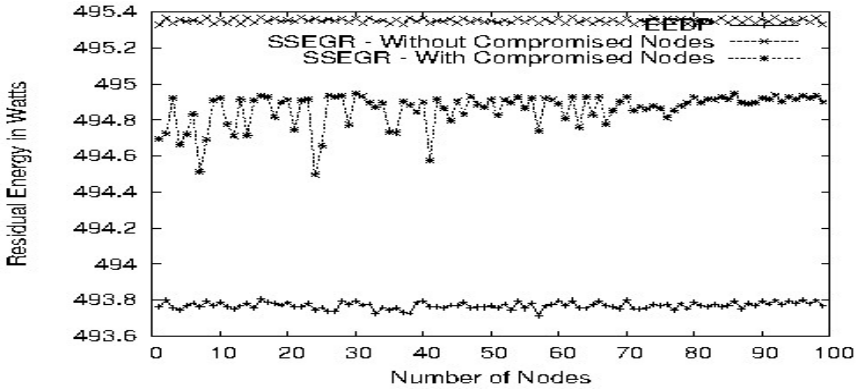

Fig. 10:Comparison of the Residual Energy with increase in the Nodes for Various Schemes.

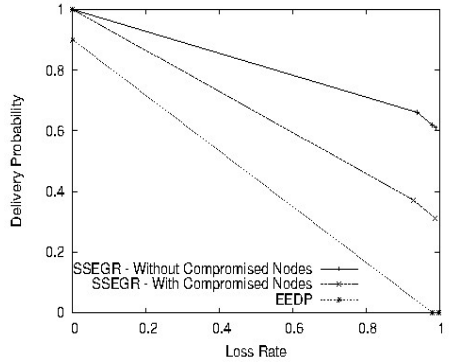

Fig. 11: Comparison of Delivery Probability with increase in Loss Rate for Various Schemes.

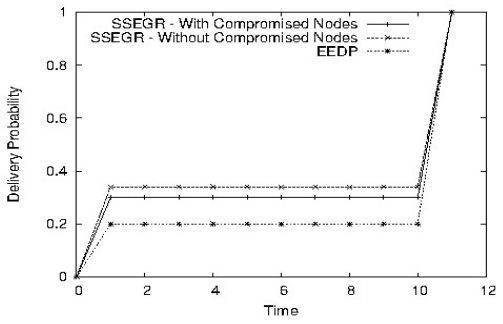

Fig.12: Comparison of Delivery Probability with increase in Time for Various Schemes.

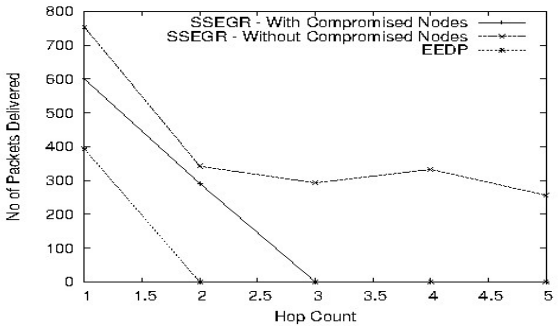

Fig. 13: Comparison of Number of Packets Delivered for Different Hop Counts.

X. Conclusions

In this paper, we propose a Secure Single Copy Energy Efficient Geographical Routing (SSEGR) algorithm for event driven WSNs to detect the event and send the information to the base station. Timeliness reliability is preserved in the process. Cluster head exchanges information with its neighboring nodes and decides about the occurrence of an event. Local broadcast of the event move towards the base station; simultaneously global broadcast is activated. Local broadcast ensurers data delivery to the next node (node to node) safely, while global algorithm takes care of sender base station (end-to-end) connectivity. In order to improve reliability and non receipt of acknowledgment then, a copy of the data is transmitted through another path. Simulation results shows that minimum energy is utilized by the nodes to perform the task as multi-copy of data is avoided.

Table 2: Simulation Parameters

Simulator	NS3
Duration	10 Sec
Sample Rate	1 sec
Area	1000m x 1000m
Radio Range	300m
Thres Dis	175m
Thres temp	75 Deg. C
Thres pres	675 mmHg
Thres smoke	40 mg/L

All the nodes play double role of data collection and routing. Since greedy technique is used to take the packet to the next hop, energy management is difficult. Critical nodes are distributed in the 1st and 2nd level of the deployment. In SSEGR algorithm all nodes works as cluster head as well as cluster members, this reduces the effect of overloading and redundant usage of energy. The proposed model improves the delivery probability. Future work will be carried out to improve the balance of load.

References

[1]. M Ozaki, Y. Adachi, Y. Iwahori, and N. Ishii, Application of fuzzy theory to writer recognition of Chinese characters, International Journal of Modelling and Simulation, 18(2), 1998, 112-116. Note that the journal title, volume number and issue number are set in italics.

[2]. Xiaonan Wang and Huanyan Qian, Constructing a 6LoWPAN Network Based on a Cluster Tree, IEEE Transactions on Vehicular Technology, 61(3), 2012, 1398-1405,

[3]. Matteo Lucchi and Marco Chiani, Distributed Detection of local Phenomena with Wireless Sensor Networks, Proc. IEEE ICC Conf. 2010, 1-6.

[4]. AVU Phani Kumar, Adi Mallikarjuna Reddy V and D Janakiram, Distributed Collaboration for Event Detection in Wireless Sensor Networks, Proc. 3rd International Workshop on Middleware for Pervasive and Ad-hoc Computing (MPAC), 2005, 1-8.

[5]. Brad Karp and H T Kung, GPSR: Greedy Perimeter Stateless Routing for Wireless Network, Proc. 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), 2000, 243-254.

[6]. Tain He, John A Stankovic, Chenyang Lu and Tarek Abdelzaher, SPEED : A Stateless Protocol for Real-Time Communication in Sensor Networks, Proc. 23rd International Conference on Distributed Computing Systems (ICDCS), 2003, 46-55.

[7]. Yogesh Sankarasubramanaiam, Ozgur B Akan and Ian F Akyildiz, ESRT: Event-to-Sink Reliable Transport in Wireless Sensor Networks, IEEE/ACM Transactions on Networking, 2002 , 38(4), 393-422.

[8]. K D Kang, K Liu and N Abu Ghazaleh, Securing Geographical Routing in Adhoc and Wireless Sensor networks, In EURASIP Journal on Wireless Communications and Networking - Special Issue on Signal Processing-Assisted Protocols and Algorithms for Cooperating Objects and Wireless Sensor Networks Archive, 2010, Article 10.

[9]. S Thrasyvoulos, K Psounis and C S Raghavendra, Single Copy Routing in Intermittently Connected Mobile Networks, Proc. First Annual IEEE Communications Society Conference Sensor and Ad Hoc Communications and Networks (IEEE SECON), 2004, 235-244.

[10]. S Thrasyvoulos, K Psounis and C S Raghavendra, Efficient Routing in Intermittently Connected Mobile Networks: The Single Copy Case, IEEE/ACM Transactions on Networking, 2008, 16(1), 63-76.

[11]. Chris Karlof and David Wagner, Secure Routing in Wireless Sensor Networks: Attacks and Counter Measures, Proc. First IEEE International Workshop on Sensor Network Protocols and Applications, 2003, 113-127.

[12]. Bo Yu and Bin Xiao, Detecting Selective Forwarding Attacks in Wireless Sensor Networks, Proc. 20th International Symposium on Parallel and Distributed Processing(IPDPS-2006), 2006, 351-357.

[13]. Lulu Liango, Deyun Gao, Hongke Zhang and W W Yang, Efficient Event Detecting Protocol in Event-Driven Wireless Sensor Networks, IEEE Journal on Sensors, 12(6), 2012, 2328-2337.

[14]. Reza Curtmola and Cristina Nita-Rataru, BSMR: Byzantine-Resilient Secure Multicast Routing in Multihop Wireless Networks, IEEE Transactions on Mobile Computing, 8(4), 2009, 445-459.

[15]. T Q Quek, D Darclari and M Z Win, Energy Efficiency of Dense Wireless Sensor Networks: To Cooperate or not to Cooperate, IEEE Journal on Selected Areas in Communications, 25(2), 2007, 459-470.

[16]. Feilong Tang, Minyi Guo, Minglu Li, Cho-Li Wang and Mianxiong Dong, Secure Routing for Wireless Mesh Sensor Networks in Pervasive Environments, International Journal of Intelligent Control and Systems, 12(4), 2007, 293-306.

[17]. Roy S, Conti M, Setia S and Jajodia S, Secure Data Aggregation in Wireless Sensor Networks, IEEE Transactions on Information Forensics and Security, 7(3), 2012, 1040-1052.

[18]. Nicholas Hubbell and Qi Han, DRAGON: Detection and Tracking of Dynamic Amorphous Events in Wireless Sensor Networks, IEEE Transactions on Parallel and Distributed Systems, 23(7), 2012, 1193-1204.

[19]. Arif Selcuk Uluagac, Raheem A. Beyah, Yingshu Li, and John A. Copeland, VEBEK: Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks, IEEE Transactions on Mobile Computing, 22(12), 2010, 994-1007.

[20]. Fengyuan Ren, Jiao Zhang, Tao He, Chuang Lin, and Sajal K. Das, EBRP: Energy-Balanced Routing Protocol for Data Gathering in Wireless Sensor Networks, IEEE Transactions on Parallel and Distributed Systems, 22(12), 2011, 2108-2125.

[21]. Kui Ren, Kai Zeng, and Wenjing Lou, Secure and Fault-Tolerant Event Boundary Detection in Wireless Sensor Networks, IEEE Transactions on Wireless Communication, 7(1), 2008, 354-363.

[22]. Jing Shi, Rui Zhang, and Yanchao Zhang, A Spatiotemporal Approach for Secure Range Queries in Tiered Sensor Networks, IEEE Transactions on Wireless Communication, 10(1), 2011, 264-273.

[23]. Byoung-Dai Lee and Kwang-Ho Lim, An Energy-Efficient Hybrid Data-Gathering Protocol Based on the Dynamic Switching of Reporting Schemes in Wireless Sensor Networks, IEEE Systems Journal, 6(3), 2012, 378-387.

[24]. Yu Wang, Xiang-Yang Li, Wen-Zhan Song, Minsu Huang, and Teresa A. Dahlberg, Energy-Efficient Localized Routing in Random Multihop Wireless Networks, IEEE Transactions on Parallel and Distributed Systems, 22(8), 2011, 1249-1257.

[25]. Haibo Zhang and Hong Shen, Energy-Efficient Beaconless Geographic Routing in Wireless Sensor Networks, IEEE Transactions on Parallel and Distributed Systems, 21(6), 2010, 881-896,

[26]. http://en.wikipedia.org/wiki/Geographic_routing

[27]. Qu Shi, Power Management in Networked Sensor Radios - A Network Energy Model, IEEE Sensors Application Symposium, San Diego, California, USA, 2007, 6-8.

[28]. www.nsnam.org/

[29]. http://www.nsnam.org /docs/release/3.2/ tutorial/tutorial_8.html

[30]. http://www.nsnam.org/ developers/tools/waf/