INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
ISSN 1841-9836, 12(6), 854-870, December 2017.

SHRP - Secure Hybrid Routing Protocol over Hierarchical Wireless Sensor Networks

B. Muthusenthil, H. Kim

Balasubramanian Muthusenthil
1. Information Security Research Institute,
Wookyoung Information Technology,
Daegu, South Korea.
2. Computer Science and Engineering,
Valliammai Engineering College, India.
bmssen@gmail.com

Hyunsung Kim*
1. Dept. of Mathematical Sciences,
University of Malawi, Malawi
2. Dept. of Cyber Security,
Kyungil University, Korea
*Corresponding author: kim@kiu.ac.kr

Abstract: A data collection via secure routing in wireless sensor networks (WSNs) has given attention to one of security issues. WSNs pose unique security challenges due to their inherent limitations in communication and computing, which makes vulnerable to various attacks. Thus, how to gather data securely and efficiently based on routing protocol is an important issue of WSNs. In this paper, we propose a secure hybrid routing protocol, denoted by SHRP, which combines the geographic based scheme and hierarchical scheme. First of all, SHRP differentiates sensor nodes into two categories, nodes with GPS (NG) and nodes with antennas (NA), to put different roles. After proposing a new clustering scheme, which uses a new weight factor to select cluster head efficiently by using energy level, center weight and mobility after forming cluster, we propose routing scheme based on greedy forwarding. The packets in SHRP are protected based on symmetric and asymmetric cryptosystem, which provides confidentiality, integrity and authenticity. The performance analyses are done by using NS2 and show that SHRP could get better results of packet loss rate, delivery ratio, end to end delay and network lifetime compared to the well known previous schemes.
Keywords: Wireless Sensor Network (WSN), routing protocol, information security, anonymity, greedy forwarding.

1 Introduction

Wireless sensor networks (WSNs) are complex distributed system which comprises of large number of tiny wireless sensor nodes. These sensor nodes are widely deployed over a geographical area for monitoring and observe data in various ambient conditions. This real time data could be used to design various applications with intelligence. WSN is a technology which becomes more mature and is gaining momentum as one of the enabling technologies for the future Internet. The major applications of WSN focus predictive maintenance, intelligent buildings, enhanced safety & security, smart home, health care and disaster management etc. The characteristics of WSN such as rapid deployment, self-organization and fault tolerance make a very promising sensing technique for military applications [2, 10]. WSN plays a dominant role and lots of researches and practical applications have been contributing to improve in terms of device size, date rate, energy etc. But the main bottleneck is based on energy factor. Since WSN operates on resource constrained environment, either changing or recharging batteries is an unmanageable task. Even the failure of single node due to low energy can prostrate the entire network. This problem forced researchers for developing an energy efficient protocol at network level [33]. At the network level various energy efficient routing protocols were developed [8, 9, 28]. Mainly the routing protocols in WSN are classified in three main categories: data centric protocols, geographic based protocols, heterogeneous protocols and hierarchical protocols. Recently, heterogeneous wireless sensor network (HWSN) routing protocols have drawn more and more attention. Various HWSN routing protocols have been proposed to improve the performance of HWSNs like EDFCM, MCR, EEPCA, LEACH and SEP. In SEP, the cluster head of the advanced node frequently becomes the cluster head than the normal node [9].

This paper mainly proposes a secure hybrid routing protocol (SHRP) which combines the concepts of geographic based and hierarchical. SHRP is consisted of two phases (i) clustering and cluster head selection phase (ii) secure routing phase.

SHRP uses a weight factor to select cluster head by considering energy level, center weight and mobility after clustering. Secure routing phase is designed based on greedy forwarding and the packets are protected based on symmetric and asymmetric cryptosystem. Thereby the routing scheme could provide confidentiality, integrity and authenticity. WSN is composed of a set of clusters. In each cluster, a node called cluster head (CH) and remaining sensor nodes are called as cluster member nodes (CM). The role of each CH is to carry out the following three roles. The first role is to gather sensed data from the cluster nodes periodically and aggregates the data to remove redundancy among correlated values [30]. The second role is to generate a time division multiple access (TDMA) schedule in which sensor nodes receive a time slot for data transmission. The third role is to transmit the aggregated data to the destination by using secure routing. Hence the lifetime of CH would be a very short span of time performs all three roles and it becomes essential to shift the cluster head periodically in a well-structured manner.

In SHRP,

(1) *a novel cluster head selection scheme is proposed between the sensor nodes based on the three factors center weight, residual energy and mobility factor*, and

(2) *secure routing scheme is designed. The performance analysis by varying the percentage of nodes with GPS (NG) and nodes with antenna (NA) is done using NS2 and shows results of the parameters like packet delivery ratio, control overhead, percentage of attacks and energy consumption varies in SHRP.*

This paper is organized as follows: Section 2 discusses about related works. Section 3 proposes our network model and proposed system in detail and devises a new secure hybrid routing protocol. Performance analysis and results are provided in Section 4. Section 5 concludes with future direction of this research.

2 Related work

This section discusses on the various clustering schemes, cluster head selection schemes and secure routing schemes over WSNs [5, 9].

Baker et al. proposed linked cluster algorithm (LCA) mainly focuses on forming an efficient network topology to handle mobility of nodes [5]. Xu et al. proposed random competition based clustering (RCC) applicable to WSN which applies "first declaration win" rule [29]. Nagpal et al. proposed clubs algorithm in which clusters are formed by local broadcast and converge in time proportional to the local density of nodes [19]. Bandyopadhyay et al. proposed energy efficient hierarchical clustering (EEHC) with the objective of minimizing the network lifetime [6]. Heinzelman et al. proposed low energy adaptive clustering hierarchy (LEACH) which is one of the popular clustering algorithm in which clusters are formed based on received signal strength and uses the cluster head as routers [11,12]. LEACH obtains energy efficiency by partitioning the nodes into clusters which comprises of setup phase and steady state phase. During setup phase the cluster head selection process is based on predetermined probability, and steady state phase is for data transmission. Wang et al. proposed clustering scheme based on queries and attributes of data [27]. Mostafaei et.al [18] presents an algorithm based on Imperialist Competitive algorithm for improving the network lifetime in WSN by diving the nodes into various cover-sets.

Alasem et al. [3] proposed a location based energy-aware reliable routing protocol (LEAR) for WSN based on enhanced greedy forwarding (EGF) protocol which selects the nearest node to be active node based on its distance but it practically fails. LEACH also does the cluster head selection process but it is based on predetermined probability does not considered the energy efficiency for cluster head selection. LEACH-centralized (LEACH-C) uses centralized algorithm for the cluster head selection where the base station collects the position and energy level of the sensor nodes and the node having greater energy than average energy of all sensor nodes would be elected as cluster head. Since this approach only considers the energy level of sensor nodes while selecting the cluster head, there may be a greater probability of elected cluster head is far away from base station which consumes more energy for the communication between base station and cluster head. Mehmood et.al [16] proposes LEACH-VH for improving the performance of LEACH in which introducing the concept of Vice Cluster Head (VH) to support CH but it leads to additional energy for electing VH. Younis et al. presented hybrid energy-efficient distributed clustering (HEED) protocol, which periodically selects cluster head according to their residual energy [31]. But the disadvantage is the authors do not make any assumptions about infrastructure or node capabilities, other than the availability of multiple power levels in sensor nodes. However, HEED supports two-level hierarchy. Ming et al. proposed a new energy-efficient dynamic clustering scheme where each node estimates the number of active nodes in real-time and computes its optimal probability of becoming a cluster head by monitoring the received signal power from its neighbor nodes [10]. Jung et al. proposed a cluster based energy-efficient forwarding scheme which uses the binary exponential back off algorithm for cluster head selection [14].

Han [9] proposes heterogeneous cluster-based protocols which has ability to manage the clusters and member nodes for better balance energy consumption of the nodes in the whole network whereas it does not satisfy for unequal distribution of clusters. Song [24] proposes a heterogeneous sensor network to improve the efficiency of network coverage but optimization needs to be addressed. Ndiaye et al. [20] proposed that Software Defined Networking (SDN) provides a promising solution in flexible management WSNs by allowing the separation of the control logic from the sensor nodes/actuators [17]. The advantage with this SDN-based management in WSNs is that it enables centralized control of the entire WSN making it simpler to deploy network-wide management protocols and applications on demand.

The cluster head selection algorithms described above is considering the two important parameters such as distance among the nodes and residual energy of the nodes. The proposed solution uses different approach from the previous where cluster head selection process is done based on the weight factor of center weight, residual energy and mobility of each node.

Bohge et al. proposed secure hierarchical routing protocol by using TESLA certificates for authentication [7]. But it cannot prevent intruders from coming into the network and sending packets and cannot protect against eavesdropping. Tubaishat et al. proposed a secure routing protocol uses the symmetric key cryptography and proposed a group key management scheme and drawback associated with this protocol is that, while changing the CH all group key i.e. inter-cluster and intra-cluster key should have to compute once again, which is a cumbersome task [26]. Parno et al. proposed LHA-SP on securing heterogeneous hierarchical WSNs uses the symmetric key scheme Authentication and confidentiality is maintained by shared pairwise key but it deals with orphan node problem [23]. Oliveria et al. proposed FLEACH, a protocol for securing node to node communication uses random key pre-distribution scheme with symmetric key cryptography but it is vulnerable to node capturing attack [22]. Ibriq et al. proposed a secure hierarchical energy efficient routing protocol (SHEER) which provides secure communication at the network layer which uses HIKES a secure key transmission protocol and symmetric key cryptography [13].

Leao et al. proposed an Alternative-Route Definition (ARounD) communication scheme for WSNs. The underlying idea of ARounD is to setup alternative communication paths between specific source and destination nodes, avoiding congested cluster-tree paths [15].

Srinath et al. proposed cluster based secure routing protocol which uses both public key (in digital signature) and private key cryptography [25]. This protocol deals with interior adversary or compromised node but it requires high computational requirement (use of public key cryptography), which is not efficient for the WSNs. Oliveira et al. proposed Sec-LEACH an efficient solution for securing communications uses random-key pre distribution and μTESLA for secure hierarchical WSN with dynamic cluster formation [21]. Quan et al. proposed secure routing protocol cluster-gene-based (SRPBCG) for WSNs [34]. Biological 'gene' as encryption key but it only deals with the adversary's attack and compromised nodes but computation and communication burden are more in this protocol. Adnan et al. [1] proposed a Secure Region-Based Geographic Routing Protocol (SRBGR) to increase the probability of selecting the appropriate relay node. By extending the allocated sextant and applying different message contention priorities more legitimate nodes can be admitted in the routing process but it fails when increasing number of nodes with different scenarios of network terrain.

3 SHRP: Secure hybrid routing protocol

This section proposes a novel secure hybrid routing protocol (SHRP) in WSN. We differentiate sensor nodes into two categories: nodes with GPS (NG) and nodes with antennas (NA). In order to propose SHRP, we need to undergo two phases: (1) clustering and cluster head selection and (2) secure routing. In Phase 1, clustering is done based on any one of the best approaches from the previous clustering schemes. However the clustering approach should satisfy that the percentage of NG must be at least three nodes in each cluster in order to support position requirement from each node. After that the cluster head selection process is done based on the weight factor of center weight, residual energy and mobility of each node. In phase 2, secure routing is designed where the packets are protected by using symmetric and asymmetric cryptosystem to support confidentiality, integrity and authenticity.

The network architecture is composed of CH and CM as entities:

- *Cluster head* (CH_i): It is node which acts as a coordinator of each cluster. We assume that NA only could be a candidate of cluster head. Any NA nodes in a cluster could be selected as the cluster head which has maximum weight factor and but with less mobility factor.

- *Cluster member* (CM_i): It is a node in a WSN is capable of performing some processing, gathering sensory information and communicating with cluster head in the network. Any NA or NG nodes could be member nodes in each cluster which is attached with CH exclusively.

Based on these assumptions, a transmission model between a source node (CM_S) and a destination node (CM_D) can be designed as follows:

Table 1: Notations

Notation	Meaning
NG	Nodes with GPS
NA	Nodes with antennas
CH_i	Cluster head i
CM_S	Cluster member source
CM_D	Cluster member destination
μ_i	Weight factor of node i
C_i	Center weight of node i
ER_i	Residual energy of node i
M_i	Mobility of node i
N_{mid}	Center of each cluster
$E_i(0)$	Initial energy level of node i
$E_i(T)$	Initial energy level of node i at time T
R_{REQ}, R_{REP}	Route request and route reply message
$AE(K, M)$	Asymmetric key encryption function with 2 inputs of key K and message M
$AD(K, M)$	Asymmetric key decryption function with 2 inputs of key K and message M
$SE(K, M)$	Symmetric key encryption function with 2 inputs of key K and message M
$SD(K, M)$	Symmetric key decryption function with 2 inputs of key K and message M
$H()$	Secure hash function
PR_D, PU_D	Private-public key pair for destination
PR_S, PU_S	Private-public key pair for source
ID_S, ID_D	Real identities for source and destination
$AID_S, , AID_D$	Amplified identities for source and destination
SK_S	Session key generated by source
T_i	Time stamp for node i
EN_S, EN_D	Encrypted messages by source and destination
MAC_S, MAC_D	Message authentication codes for source and destination
AU_S, AU_D	Authenticated values by source and destination
$\|\|$	Concatenation operator
SF	Security field
Q	Query message
M_{ID}	Message ID

Table 2: Recommended clustering algorithms

Algorithms Required Parameters	Cluster overlapping	Location awareness
LCA	No	Required
Adaptive clustering	No	Required
RCC	No	Required
GS3	Low	Required
EEHC	No	Required
DWEHC	No	Required
Attribute based clustering	No	Required

- If CM_S is located within the distance r_s from CM_D, CM_S transmits the packet to CM_D via the cluster head CH_S.
- When CM_D is outside of the transmission range from CM_S, the packet is forwarded to the intermediate cluster heads in the direction of CM_D.

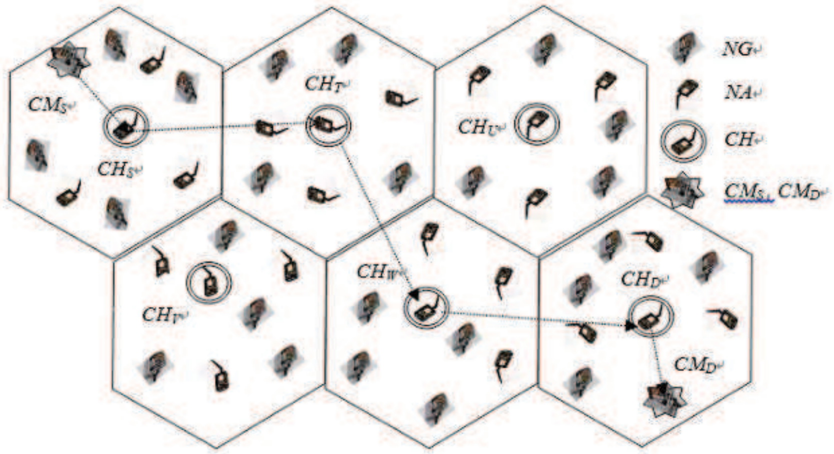

Figure 1: Network configuration

3.1 Clustering and cluster head selection phase

Clustering

WSN involves large number of sensors for which clustering is an effective and efficient way for managing high volume of nodes. There are many clustering schemes, which were proposed by various researchers based on different categories. Many of the clustering algorithms are given in related works [8, 10]. This objective of clustering is out of scope to our research but the research objective we tabulated few clustering schemes which suits for our network model . Therefore clustering is done based on any of the clustering approaches in in Table 2. However, the clustering should satisfy that the percentage of NG nodes must be at least three nodes in each cluster in order to support requisition requirement from each node.

Cluster head selection

As we mentioned at the network initialization and transmission model, each node could get their location information with the help of NG nodes. The cluster head selection process is done based on the parameters of weight factor (μ_i) along with center weight (C_i), residual energy (ER_i) and mobility (M_i) of each node i. The Weight factor of the node is defined as the weight assigned to a node based on its residual energy and mobility, in order to give less or more importance to the other nodes in the cluster. Weight factor of the node i (μ_i) is computed by (1).

$$\mu_i = (x_1 * C_i) + (x_2 * ER_i) - (x_3 * M_i), \quad (1)$$

where x_1, x_2 and x_3 are threshold values such that $x_1 + x_2 = 1$. x_3 is a deduction factor due to its mobility.

Table 3: Cluster head selection message format

Node ID	Weight factor (μ_i)	Node mobility (M_i)

Let N_{mid} be the center of each cluster which can be determined by help of NG nodes. The center weight (C_i) of the node i is computed by using (2).

$$C_i = N_{mid} * \alpha, \tag{2}$$

where α is the distance from the border node of its cluster to N_{mid}, which ranges from 0 to 1 depending upon the location.

Let $E_i(0)$ be the initial energy level (ER_i) of the node i. At a time period T, the energy consumed by the node i ($E_i(T)$) is computed by using (3).

$$E_i(T) = n_{tx} * \beta + n_{rx} * \gamma, \tag{3}$$

where n_{tx} and n_{rx} are the numbers of data packets transmitted and received by the node i at time T, respectively. β and γ are in the range $(0, 1)$ to measure energy consumption level.

The residual energy of the node $i(ER_i)$ at time T is computed using (4).

$$ER_i = E_i(0) - E_i(T). \tag{4}$$

The node mobility (M_i) of node i is computed using (5).

$$M_i = \frac{\sqrt{(u_2 - u_1)^2 + (v_2 - v_1)^2}}{T_2 - T_1}, \tag{5}$$

where (u_1, v_1) and (u_2, v_2) are the coordinates of the node i at time T_1 and T_2, respectively.

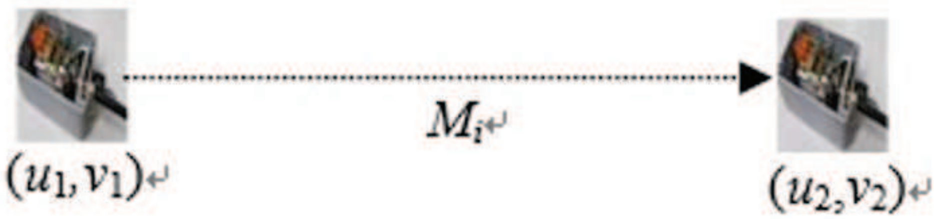

Figure 2: Node mobility

The steps involved in cluster head selection are as follows.

1. When the nodes are deployed in a WSN, all the nodes compute μ_i and broadcast cluster head selection message to its neighbors, which follows the format of Table 3. It includes the parameters such as node ID, weight factor and node mobility.

2. When node receives the message, it forms a member list (ML), and checks whether it has the maximum weight factor $\mu_{\max}$ by using the obtained ML.

3. Node with $\mu_{\max}$ is elected as cluster head (CH_i) as shown in Figure 1

4. If there are more than one node with $\mu_{\max}$ value, less mobility factor node is selected as the cluster head and it transmits cluster head election message (CH_{Elec}), which contains ID_{CHi} to every nodes in the cluster.

If a node in ML needs to leave from the cluster, it sends leave request (L_{Req}) message to CH_i. CH_i broadcasts the updated ML to every member nodes which removes the node from ML. Similarly, when a node in ML needs to join into the cluster, it sends join request (J_{Req}) message to CH_i. CH_i broadcasts the updated ML to every member nodes which adds the node into ML.

3.2 Secure routing phase

The task of secure routing is to form route from source CM_S to destination CM_D by sending packets while complying with the condition of that CM_S is informed about the position of CM_D. The secure routing is described as the following steps:

1. When CM_S wants to transmit a route construction request with a query to CM_D, it invokes form_message(), unicasts R_{REQ} to its CH_S and stores M_{ID} in its route cache termed as session table (ST), which helps to distinguish the respective R_{REQ} while receiving R_{REP}.

Table 4: Route request message format

Message ID (M_{ID})	Source ID (AID_S)	Destination ID (ID_D)	Location of CH_i (NL)	Destination location (L_D)	Security field (SF)	Query (Q)

2. When CH_S receives R_{REQ}, it checks L_D and invokes request_route_CH(R_{REQ}).

function REQUEST_ROUTE_CH(R_{REQ})
  if L_D is within ML or ID_D is member of CH_S **then**
    Send R_{REQ} directly to CM_D
  else
    Send R_{REQ} directly to CM_i towards direction of L_D
    do
      CH_i broadcast to nearest NL towards L_D
    while (not reach to CH_D)
  end if
end function

function FORM_MESSAGE()
  CM_S generates a session key K_S and forms a message $M_S = ID_S \| ID_D \| K_S \| PU_S \| T_S$ with T_S
  Encrypts M_S with PU_D by applying asymmetric encryption $EN_S = AE(PU_D, M_S)$
  Computes $MAC_S = H(EN_S \| K_S)$
  Computes authenticated value $AU_S = AE(PR_S, T_S)$
  Sets $NL = NULL$
  returns (EN_S, MAC_S, AU_S)
end function

3. If R_{REQ} reaches to MN_D, CH_D invokes verify_message() and respond_route(R_{REP}) to return back R_{REP} to CH_S

function VERIFY_MESSAGE()
  CM_D decrypts EN_S by using PR_D and retrieves $M'_S = ID'_S \| ID'_D \| K'_S \| PU'_S \| T'_S$ by using $AD(PR_D, EN_S)$
  Computes $MAC'_S = H(EN_S \| K'_S)$
  Checks the validity MAC_S by comparing with MAC'_S
  Checks authenticity of source by $AD(PU_S, AU_S)$

CM_D forms acknowledgement message $M_A = ID_S \| ID_D \| K_S \| PU_D \| T_D$
    if verification is successful **then**
        Compute $EN_D = SE(K_S, M_A)$
        Computes $MAC_D = H(EN_D \| T_D)$
    end if
    $AU_D = AE(PR_D, T_D)$ **return** EN_D
end function
function RESPOND_ROUTE_$CH(R_{REP})$
    if L_S is within ML or ID_S is member of CH_D **then**
        Send R_{REP} directly to CM_S
    else
        Send R_{REP} directly to CM_i towards the direction of L_S
        do
            CH_i broadcast to nearest NL towards L_S
        while (not reach to CH_S)
    end if
end function

4. If CM_S receives R_{REP}, the secure routing process is successful.

4 Analysis

This section provides performance analysis and security analysis after providing simulation results on SHRP. We used NS2 to provide simulation results of SHRP, which uses parameters of Table 5. Simulations were carried out based on LEACH, EEHC and SHRP [**?**, **?**]

Table 5: Simulation parameter

Parameters	Values
Initial energy of nodes E_{unit}	$0.5J$
Amplification coefficient of the free space model E_{fs}	$10pJ \cdot m^2/b$
Amplification coefficient of the multipath transmission model E_{amp}	$0.0013pJ \cdot m^2/b$
Table data fusion rate E_{DA}	$5nJ/b$
Circuit loss E_{elec}	$50nJ/b$
Clustering probability of nodes p	0.05
Data packet length	$4000b$
Control packet length	$80b$

4.1 Performance analyses

Figure 3 and Figure 4 show the packet loss rate results depending on the different number of nodes to form clusters based on various clustering techniques.

SHRP minimizes the packet loss rate approximately 3.27% in the number of NG nodes and 3.34% in the number of NA nodes than EEHC. Furthermore, it reduces the rate approximately 40.02% in NG nodes and 47.06% in NA nodes than LEACH.

SHRP has less end to end delay compared to EEHC and LEACH as shown in Figure 5 and Figure 6.

As shown in Figure 5 and Figure 6, SHRP has better performance than LEACH and EEHC

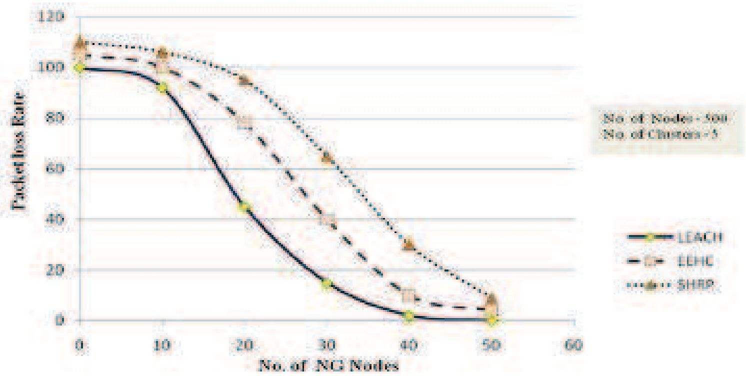

Figure 3: Packet loss rate depending on changes of the number of NG nodes

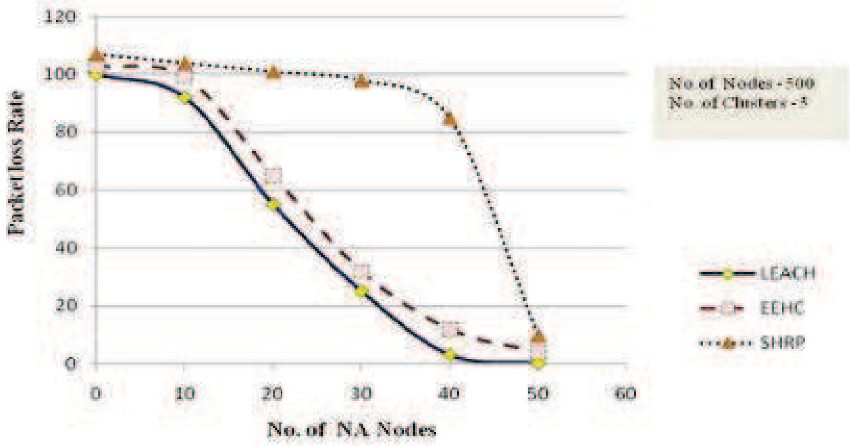

Figure 4: Packet loss rate depending on changes of the number of NA nodes

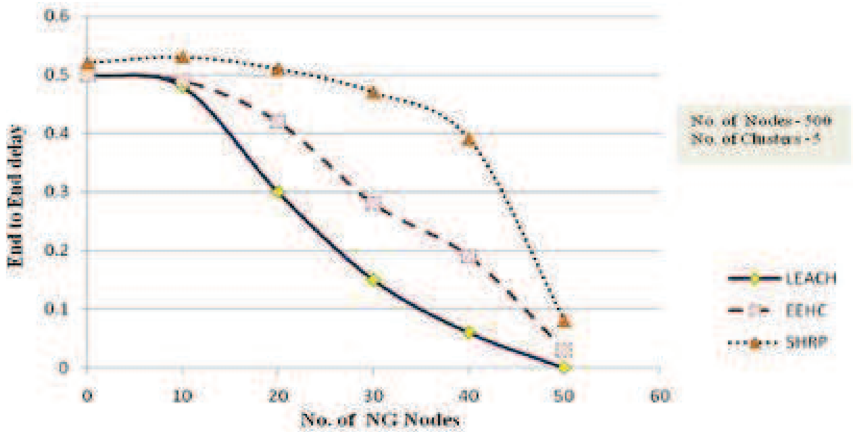

Figure 5: End to end delay depending on changes of the number of NG nodes

for the number of NG and NA nodes changes. Hence the delivery latency of SHRP in the number of NG nodes changes is higher than the other case.

Figure 7 and show the variations on the three schemes and they characterize that incurs approximately 97.9% packet delivery ratio. LEACH and EEHC achieve the packet delivery ratio

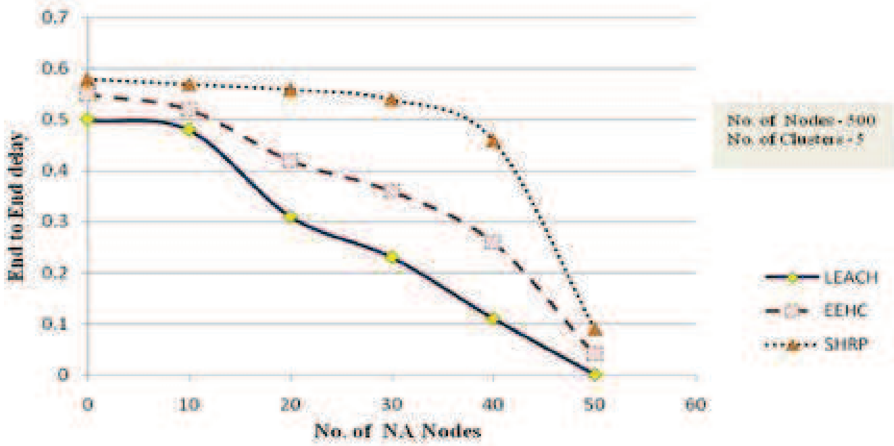

Figure 6: End to end delay depending on changes of the number of NA nodes

in average of 95.2% and 91%, respectively. From Figure 8 the SHRP in number of NA nodes incurs 98.2% (approx) delivery of data packets and results in better rate compared to delivery rate in NG nodes.

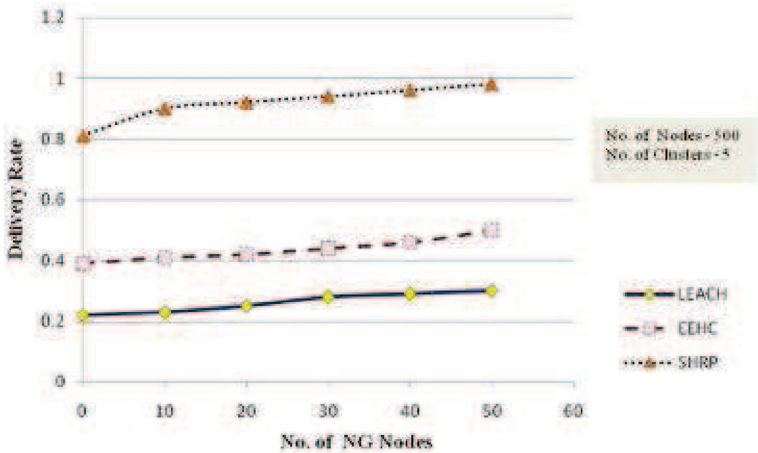

Figure 7: Delivery ratio depending on changes of the number of NG nodes

From Figure 9 and Figure 10 it is understood that SHRP has 32% of delay in delivering data packets. LEACH and EEHC delivery delay rate at a rate of 48% (approx) and 43.05%. Hence SHRP result has better performance than LEACH and EEHC for number of NG nodes and SHRP has 28% (approx) of delay in delivering data packets for NA nodes.Hence delivery latency of SHRP in number of NG node is high than delivery latency of SHRP in number of NA nodes.

Figure 11 and Figure 12 shows the network lifetime in number of NG nodes. SHRP has the network lifetime of 30.05% (approx). LEACH and EEHC has the network lifetime of 32.6% (approx) and 35.09% (approx).

Figure 11 and Figure 12 show the comparison of network lifetime, which shows that SHRP has longest lifetime compared to LEACH and EEHC.

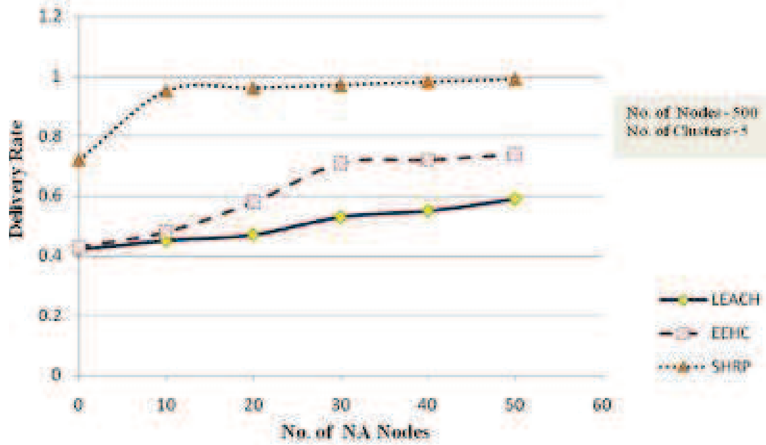

Figure 8: Delivery ratio depending on changes of the number of NA nodes

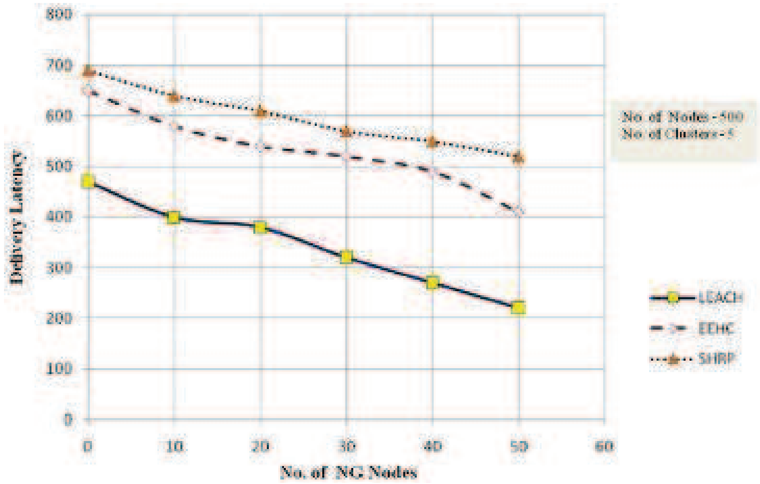

Figure 9: Delivery latency depending on changes of the number of NG nodes

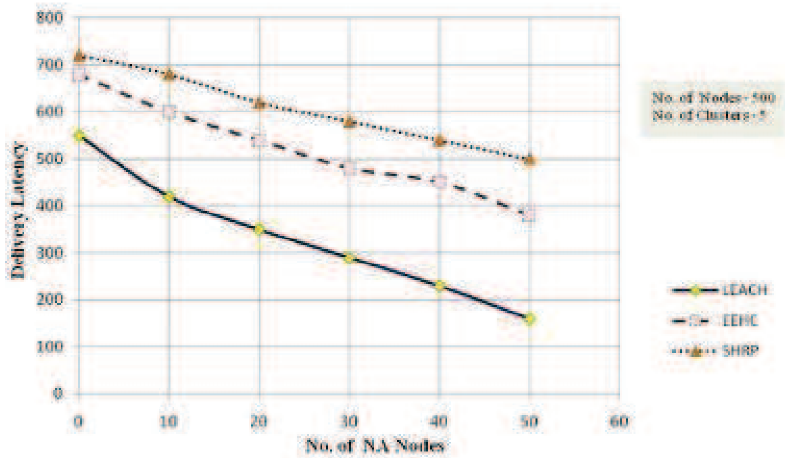

Figure 10: Delivery latency depending on changes of the number of NA nodes

4.2 Security analysis

The focus of this analysis is to ensure how secure the message transmissions in SHRP between CM_S and CM_D, which is only focused on the secure routing phase.

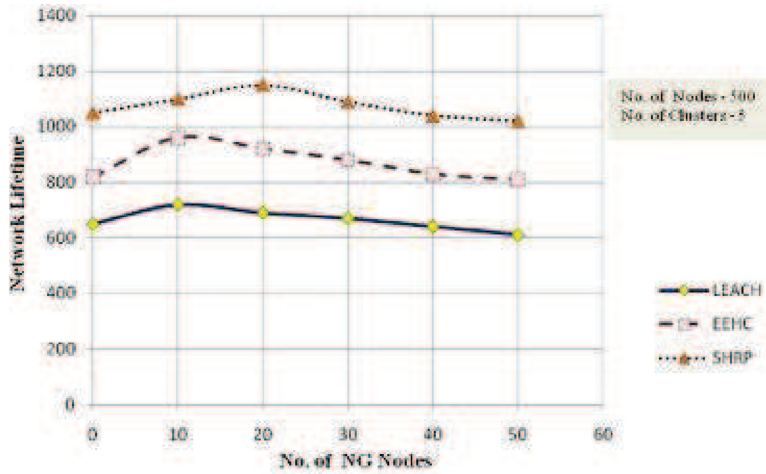

Figure 11: Network lifetime depending on changes of the number of NG nodes

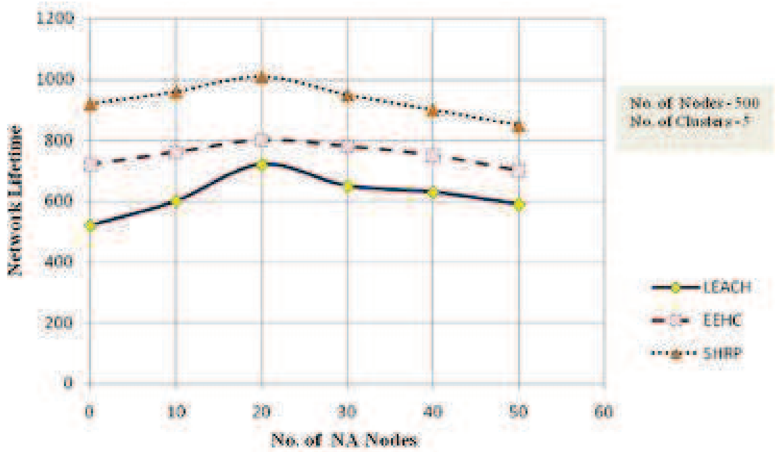

Figure 12: Network lifetime depending on changes of the number of NA nodes

Once the messages to establish route are secured, it is inferred that communications over the WSN are secure.

1. *Unlinkability/Anonymity*: SHRP achieves anonymity by using encrypted message of identities, which could provide security of ID_S. This is achieved by sending the encrypted message EN_S during route construction request message formatting. There is no way an attacker can discover the source node's real identity because no user identification information is transmitted in plain. Therefore, SHRP provides entity anonymity. Further unlinkability is provided because the timestamp T_S is protected from the preying eyes of an adversary and therefore cannot be related to a particular node by anyone other than CM_D. So, entity privacy is guarded against eavesdropper. This means the session key derived after authentication ensures privacy of end entity information like sensed data or any encrypted messages.

2. *Impersonation Attack*: An attacker may attempt to use a bogus CH_i or CM_i to impersonate the real one that the attacker has access to. As much as the attacker has no knowledge of any entity in the network due to anonymity and unlinkability properties, the attacker cannot manage to impersonate any entity in WSN with a malicious CH_i or CM_i. Even

from the transmitted message, (EN_S, MAC_S, AU_S) and (EN_D, MAC_D, AU_D) relayed between CM_S and CM_D, the attacker cannot modify them to pass authentication because he/she will need to have the secret values related to the message in order to impersonate either CM_i or CH_i to pass the counterpart's verification. This attack is difficult to materialize because the real identity of the entity is still concealed to all players in SHRP.

3. *Replay Attack*: An attacker may wish to initialize a replay attack from eavesdropped data packets of an authenticated communication between CM_S and CM_D and retransmit them at a later time as if it comes from the real entity. This attack is thwarted in SHRP because the authenticated message $EN_S = AE(PU_D, M_S)$ for route construction message contains timestamp T_S meant to be used once, so there is no way an attacker can devise a replay of any message encrypted with the related secret keys. In the same way the session key SK is unique per session and is updated after any successful secure routing procedure. So, its arguable SHRP resists against the replay attack.

4. *Man-in-the Middle Attack*: In man-in-the-middle attack, an adversary eavesdrops and intercepts the communication between or among communicating legal entities in WSN and relays authentic messages to the victims to make them that believe they are communicating confidentially. Thus, the adversary controls the whole communication sessions without knowledge of the intended entities in WSN. However this attempt though cannot succeed in SHRP because no attacker can manage to initiate the fabrication of the legal message that seems acceptable to CM_D. Since to achieve this attack, the adversary must find a means of sending verifiable components EN_S, MAC_S and AU_S in order to pretend as CM_S to CM_D. Obviously, there is no other way of forging EN_S without knowledge of the parameters of M_S. Furthermore, the extraction of MS from EN_S means the ability to solve the discrete logarithm problem that can be solved by CM_D only. Therefore the attacker will not succeed and besides the message M_S is not sent in plain, thus the attacker will not know the information targeted to CM_D. Conclusively, SHRP is resilient against impersonation attack.

5. *Mutual Authentication*: In SHRP, both end point the origin and the destination of a transmitted message authenticate and verify the counterpart, thereby providing mutual authentication. Before CM_S and CM_D can communicate securely they first share the counter part's public key. So based on the public key, the parties transmit messages authentic and verifiable only between themselves. For instance, when CM_S sends login message EN_S, MAC_S and AU_S to CM_D, it is formed in a way that only CM_D with the knowledge of the private key can extract the message. Having extracted EN_S, CM_D verifies the counterpart entity and establish a session key SK securely only after the proper authentication success. On the other hand CM_D authenticates an CM_S by checking the received MAC_S and AU_S. CM_D trust that it is communicating with an unintended party is based on the assumption that computing EN_S, MAC_S and AU_S without knowledge of $CM_D's$ private key involves solving the discrete logarithm, which is infeasible by an attacker. At the end, CM_S and CM_D mutually authenticate each other.

5 Conclusion

This paper has been proposed a secure hybrid routing protocol (SHRP), which combines the geographic based scheme and hierarchical scheme. SHRP classified sensor nodes into two categories, NG nodes and NA nodes, to put different roles in WSNs. SHRP is consisted with two phases: the clustering and cluster head selection phase and the secure routing phase. In the clustering and cluster head selection phase, SHRP selects a clustering scheme from the previous schemes to satisfy that the percentage of NG must be at least of three nodes in each cluster in order to support location requirement of each node. After that the cluster head selection process is done based on a new weight factor of center weight, residual energy and mobility of each node. In the secure routing phase, a secure routing is designed where the packets are protected by using symmetric and asymmetric cryptosystem to support confidentiality, integrity and authenticity. As shown in the performance analyses, SHRP could get better results of packet loss rate, delivery ratio, end to end delay and network lifetime compared to the well known previous schemes.

Acknowledgements

Corresponding author is Hyunsung Kim and this work was supported by the Korean Federation of Science and Technology Societies(KOFST) grant funded by the Korean government (MSIP:Ministry of Science, ICT and Future Planning) and Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

Bibliography

[1] Adnan A. I., Hanapi Z. M., Othman M. , Zukarnain Z. A. (2017); A Secure Region-Based Geographic Routing Protocol (SRBGR) for Wireless Sensor Networks, *PloS one*, 12(1), p. e0170273, 2017.

[2] Akyildiz I. F. , Su W., Sankarasubramaniam Y., Cayirci E. (2002); A survey on sensor networks, *IEEE Communications magazine*, 40(8), 102–114, 2002.

[3] Alasem R., Reda A., Mansour M. (2011); Location based energy-efficient reliable routing protocol for wireless sensor networks, *Recent Researches in Communications, Automation, Signal processing, Nanotechnology, Astronomy and Nuclear Physics, WSEAS Press, Cambridge, UK*, 2011.

[4] Almeida F. R., Brayner A., Rodrigues J. J. P. C., Maia J. E. B. (2017); Improving Multidimensional Wireless Sensor Network Lifetime Using Pearson Correlation and Fractal Clustering, *Sensors*, 17(6), E1317. doi: 10.3390/s17061317, 2017.

[5] Baker D.J., Ephremides A, Flynn J. A. (1984); The design and simulation of a mobile radio network with distributed control, *IEEE Journal on selected areas in communications*, 2(1), 226–237, 1984.

[6] Bandyopadhyay S., Coyle E. (2003): An energy efficient hierarchical clustering algorithm for wireless sensor networks, *INFOCOM 2003 - Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, 3, 1713–1723, 2003.

[7] Bohge M., Trappe W. (2003); An authentication framework for hierarchical ad hoc sensor networks, *Proceedings of the 2nd ACM workshop on Wireless security*, 79–87, 2003.

[8] Chang J.Y., Ju P.H. (2012); An efficient cluster-based power saving scheme for wireless sensor networks, *EURASIP Journal on Wireless Communications and Networking*, 2012:172, https://doi.org/10.1186/1687-1499-2012-172, 2012.

[9] Han G., Jiang X., Qian. A., Rodrigues J. J.P.C., Cheng L., (2014); A comparative study of routing protocols of heterogeneous wireless sensor networks, *The Scientific World Journal*, Article ID 415415, 1–11, 2014.

[10] Handy M.J., Haase M., Timmermann D. (2002); Low energy adaptive clustering hierarchy with deterministic cluster-head selection, *4th International Workshop on Mobile and Wireless Communications Network, 2002*, 368–372, 2002.

[11] Heinzelman W.B., Chandrakasan A.P., Balakrishnan H. (2002); An application-specific protocol architecture for wireless microsensor networks, *IEEE Transactions on wireless communications*, 1(4), 660–670, 2002.

[12] Heinzelman W. B., Chandrakasan A. P., Balakrishnan H. (2000); Energy-efficient communication protocol for wireless microsensor networks, *Proceedings of the 33rd annual Hawaii international conference on System sciences, IEEE*, 1-10, 2000.

[13] Ibriq J., Mahgoub I. (2006); A secure hierarchical routing protocol for wireless sensor networks, *10th IEEE Singapore International Conference on Communication systems, ICCS 2006, IEEE*, 1–6, 2006.

[14] Jung S., Chung Y. (2007); An interest-diffused clustering routing algorithm by bitmap in wireless sensor networks, *5th ACIS International Conference on Software Engineering Research, Management & Applications, - SERA 2007, IEEE*, 697–701, 2007.

[15] Le E., Montez C., Moraes R., Portugal P., Vasques F. (2017); Alternative Path Communication in Wide-Scale Cluster-Tree Wireless Sensor Networks Using Inactive Periods, *Sensors*, 17(5), 1049, 2017.

[16] Mehmood A., Lloret J., Noman M., Song H. (2015); Improvement of the Wireless Sensor Network Lifetime Using LEACH with Vice-Cluster Head, *Ad Hoc & Sensor Wireless Networks*, 28(1-2), 1–17, 2015.

[17] Misbahuddin M., Sari R. F. (2016); Initial Phase Proximity for Reachback Firefly Synchronicity in WSNs: Node Clustering, *International Journal of Computers Communications & Control*, 12(1), 90–102, 2016.

[18] Mostafaei H., Shojafar M. (2015); A new meta-heuristic algorithm for maximizing lifetime of wireless sensor networks, *Wireless Personal Communications*, 82(2), 723–742, 2015.

[19] Nagpal R., Coore D. (1998); An algorithm for group formation in an amorphous computer, *Proc. 10th International Conference on Parallel and Distributed Computing Systems (PDCS'98)*, 1-4, 1998.

[20] Ndiaye M., Hancke G. P., Abu-Mahfouz A. M. (2017); Software Defined Networking for Improved Wireless Sensor Network Management: A Survey, *Sensors*, 17(5), pii: E1031. doi: 10.3390/s17051031, 2017.

[21] Oliveira L. B., Ferreira A., Vilaca M. A., Wong H. C., Bern M., Dahab R., Loureiro A. A. F. (2007); SECLEACH - On the security of clustered sensor networks, *Signal Processing*, 87(12), 2882–2895, 2007.

[22] Oliveira. L. B., Wong. H. C., Bern. M., Dahab. R., Loureiro. A. A. F. (2006); SecLEACH-A random key distribution solution for securing clustered sensor networks, *Fifth IEEE International Symposium on Network Computing and Applications, NCA 2006, IEEE*, 145–154, 2006.

[23] Parno B., Luk M., Gaustad E., Perrig A. (2006); Secure sensor network routing: A clean-slate approach, *Proceedings of the 2006 ACM CoNEXT conference, ACM*, 1-11, 2006.

[24] Song X. , Gong Y. , Jin D. , Li Q. , Jing H. (2017); Coverage Hole Recovery Algorithm Based on Molecule Model in Heterogeneous WSNs, *International Journal of Computers Communications & Control*, 12(4), 562–576, 2017.

[25] Srinath R., Reddy A. V., Srinivasan R. (2007); AC: Cluster based secure routing protocol for WSN, *Third International Conference on Networking and Services, 2007. ICNS., IEEE*, 45–45, 2007.

[26] Tubaishat J.M., Yin J., Panja B., Madria S. (2004); A secure hierarchical model for sensor network, *ACM Sigmod Record*, 33(1), 7–13, 2004.

[27] Wang K., Abu Ayyash S., Little T. D. C., Basu P. (2005); Attribute-based clustering for information dissemination in wireless sensor networks, *Proceeding of 2nd annual IEEE communications society conference on sensor and ad hoc communications and networks (SECON'05), Santa Clara, CA*, 2005.

[28] Wei D., Jin Y., Vural S., Moessner K., Tafazolli R, (2011); An energy-efficient clustering solution for wireless sensor networks, *IEEE transactions on wireless communications*, 10(11), 3973–3983, 2011.

[29] Xu K., Gerla M. (2002); A heterogeneous routing protocol based on a new stable clustering scheme, *MILCOM 2002. Proceedings IEEE*, 2, 838–843, 2002.

[30] Yoon M. S., Kim H., Lee S. W. (2008); Efficient dual-layered hierarchical routing schueme for wireless sensor networks, *Proceedings of International Conference on National Competitiveness and IT*, 507–511, 2008.

[31] Younis O., Fahmy S. (2004); HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks, *IEEE Transactions on mobile computing*, 3(4), 366–379, 2004.

[32] Yu M. , Leung K.K., Malvankar A. (2007); A dynamic clustering and energy efficient routing technique for sensor networks, *IEEE Transactions on wireless communications*, 6(8), 3069-3079, 2007.

[33] Zong Z., Manzanares A., Ruan X., Qin X. (2011); EAD and PEBD: two energy-aware duplication scheduling algorithms for parallel tasks on homogeneous clusters, *IEEE Transactions on Computers*, 60(3), 360–374, 2011.

[34] Zhou Q., Li J. (2009); Secure routing protocol cluster-gene-based for wireless sensor networks, *1st International Conference on Information Science and Engineering (ICISE), IEEE, 2009*, 4098–4102, 2009.