ENERGY EFFICIENT AND SECURED GEOCAST PROTOCOL IN WIRELESS SENSOR NETWORK DEPLOYED IN SPACE (3D)

Alain Bertrand Bomgni[1], Elie Tagne Fute[1], Garrik Brel Jagho Mdemaya[1], Ange Anastasie Kembouk Donfack[1] and Clementin Djamegni Tayou[1]

[1]Department of Mathematics and Computer Science, University of Dschang, Cameroun

ABSTRACT

In recent years, sensor networks are often deployed in several geographical regions to study certain phenomena. In this case, it may therefore happen that it is necessary to send a message to all the nodes of one or more regions for example to ask them to go into sleep mode. This problem is known in the literature as geographical routing (geocast). Several works have been proposed to solve this problem. In this paper we propose an energy-efficient and secured geocast protocol for a WSN deployed in space with data guarantee delivery to all nodes placed in one or more geocast regions. Our protocol consists of two major parts which are complementary and in addition of being secured, it is energy-efficient due to the fact that few messages are exchanged between the sensors during the first part of the algorithm.

KEYWORDS

Wireless Sensor Network, geocast, geocast region, security, energy consumption

1. INTRODUCTION

A Wireless Sensor Network is an ad hoc network constituted of several sensors collaborating each other in order to supervise or to collect data in a certain zone for analysis by an end user. Sensors composing the network generally have weak capacities of memory and energy, the access to the medium radio being the most expensive element in energy [1]. In these networks, security and the energy conservation are two important and necessary aspects to consider. Particularly, security allows making sure that such a network will not be subject to attacks which concern the reading, the modification and the destruction of the information whereas the energy conservation allows to extend the network lifetime since the energy of nodes sensors is extremely limited [2]. The applications of these types of networks are numerous and varied and once deployed, the sensors must work independently [3]. The protocols set up must therefore minimize the energy consumption of the sensors in order to ensure a long service life of the network.

In such systems, there is often a need to send a message to sensor nodes located in multiple geographic regions [4]. For example, in the medical field, sensors can be placed on all patients in a hospital to measure the blood pressure of each patient. Thus, by means of a computer, it is possible to send a message to all the sensors to collect the necessary data on all the patients and send them to the base station. Another example is presented in [4] in the context of smart city projects.

DOI: 10.5121/ijwmn.2018.10202

The underlying problem is the sending of a message from a source to one or multiple geographic regions; that means to all sensors located in one of those regions or to all sensors located in all those regions (geocast). Most of the works that are done to solve this problem focus on sending messages to a single node, to a set of nodes or to a single geographic region [4]. However, some are interested in geocast with several regions, but are realized in the plan and do not integrate security.

In this paper we propose a method of transmitting information that guarantees data delivery to each sensor located in one or several specific regions of a network. Indeed, we propose a protocol which is secured and energy-efficient which performs in two stages: the first stage is devoted to the clustering of the network into clusters in which CHs are elected and in the second stage we present a geocast protocol which is secured and energy-efficient.

The paper continues as follows: in section 2 we present the various works dealing with the geocast problem; in Section 3, we present our contribution to solving the problem of geocast in multiple regions; in section 4, we analyse security issues, Section 5 presents some experimental results. A conclusion with open problems ends the paper.

2. RELATED WORKS

The most obvious approach to implement the geocasting is the use of flooding. The BS sends a message to all its neighbours, who transmit it to their neighbours and so on, until all the sensors of the geocast region are affected and have the knowledge of the message. But this approach inferred several problems such as network overload, collisions, etc. In [4] a good classification is done in order to regroup the works presented in the state of the art in different categories.

2.1. Geocasting to a Set of Nodes

Several solutions in the literature support the delivery of a message from a source node to a set of destination nodes where geo-localisation of each node is known. Among these solutions, the one of Sanchez J. and al [5] called GMR protocol divides the destination group into subgroups and for each forwarding node, a minimal subset of the node's neighbours that promises most progress towards the destinations is selected as the next relay of the packet. A drawback of this protocol is that the computation of such a minimal subset is performed at all intermediate relay nodes along the routes from the source to all destinations. This is expensive especially when the network density is high and the routes are long.

Protocols presented in [5], [6], [7] and [8] consider individual destination sensors while the multi-region geocast problem considers geocast regions containing many sensors each. Moreover, these protocols have been designed for small-scale networks and for a small set of destination (whose destination have to be included in the message header).

2.2. Geocasting to a Single Region

In this case, the problem is to deliver data packets from a source to all nodes located in a particular geographical region. Thus, the protocol presented in [9] uses flooding with restricted flooding zone to deliver data packets to the geocast region. Although flooding zones reduce bandwidth usage when compared to conventional flooding, it does not scale in geographically large-scale WSN. Moreover, the protocol will fail in the presence of network partitions within the flooding zone.

In [10], authors present two algorithms: the first GFG (Geographic Forwarding-Geocast) has minimal network overhead and is ideal for dense networks. The second GFPG (Geographic-Forwarding Perimeter-Geocast) guarantees the delivery of packets to all nodes in the geocast region when the network is connected and even if the density is not large or the distribution of the nodes is irregular with obstacles. They propose to include out-region nodes in packet dissemination. GFPG uses face routing on the planar faces intersecting the region border in addition to flooding inside the region to reach all nodes.

2.3. Geocasting to Multiple Region

Few works have been done in this category especially [11], [12], [13], [14]. In [12] the work relies on flooding to discover routes to the geocast regions using "route discovery" and "route reply" messages. This approach clearly does not scale with network node density and quantity. The protocol in [14] geographically partitions the deployment area of the network into disjoint and equally sized cells, and performs geocast routing on top of these cells' managers. Again, cell management and maintenance should be considered as extra overhead for this protocol. In [4], for each forwarding node, a minimal subset of the node's neighbours that promises most progress towards the destinations is selected as the next relay of the packet; but contrary to the protocol presented in [5], this protocol performs a lighter computation only when a particular condition is violated, therefore saving processing resources. In addition, the protocol in [4] is tailored for regions located remotely from the source in geographically large-scale sensor networks.

3. Our Contribution: An Energy Efficient And Secured Geocast Protocol In Wireless Sensor Network Deployed In Space (3D)

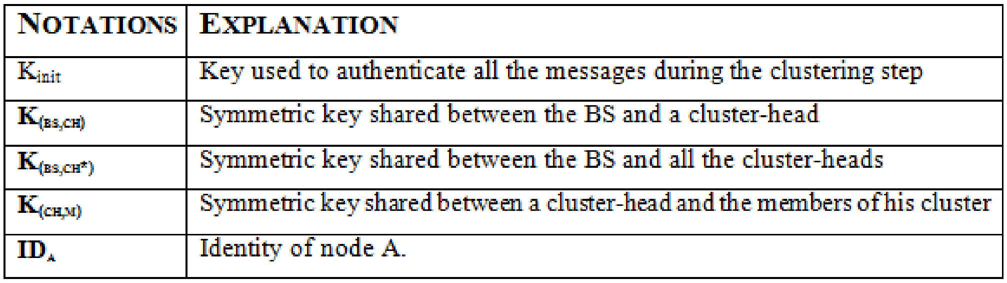
3.1 Assumptions And Notations

3.1.1 Assumptions

We consider that the stations are static and randomly deployed in space, and each station has an ID. Each station is able of being located in the space by using either the GPS(GLOBAL POSITIONING SYSTEM), or the triangulation or a system of positioning for an ad hoc network; The BS is located in the centre of the network, and it is the only station in which we can trust and that we cannot compromise. The network is sufficiently dense; thus each cluster will have at least one sensor.

3.1.2 Notations

Our notations are explained in table 1.



Notations	Explanation
K_{init}	Key used to authenticate all the messages during the clustering step
$K_{(BS,CH)}$	Symmetric key shared between the BS and a cluster-head
$K_{(BS,CH^*)}$	Symmetric key shared between the BS and all the cluster-heads
$K_{(CH,M)}$	Symmetric key shared between a cluster-head and the members of his cluster
ID_A	Identity of node A.

Table 1: Notations.

3.2 Protocol phases

After deployment, the BS computes the cryptographic parameters using an elliptic curve E(a,b,K); that is, it chooses a finite field K and an elliptic curve $y^2=x^3+a^2+b$. After that, it initializes an array T containing the identities of all the sensors and a point *P* on the curve that will be used to establish a private key between nodes. The BS generates a key K_{init} and gives to all the sensors the following values: ID, K_{init}, E(a,b,K) and P.

All the messages are coding using the key K_{init} during the clustering step.

3.3 First stage: secured clustering procedure

The BS partitions the network into clusters in a secure way using the same technique presented in [15].

3.3.1 Formation of crowns

The integer *l* is known by all the nodes, each node must read a string of $\log_2(l)$ bits determining the identity of its crown. The formation of crowns is secured using the K_{init} key.

3.3.2 Formation of horizontal sections

The integer *m* is known by all the nodes, each node must read a string of $\log_2(m)$ bits determining the identity of its horizontal section. Communications are secured using the K_{init} key. The value of α is given by the theorem 1.

Theorem 1: In order to permit to each sensor to communicate with his neighbours in one hop, the BS broadcasts emissions of angle α such as $\sin(\alpha) = 2/R^2_c$. where R^2_c is the communication radius of a sensor.

Proof: Let us consider the figure 1; the biggest clusters are those who are far away from the BS. Thus, we will use the last crowns to determine the value of α.
Let R_i be the radius of the internal sphere and R_{i+1} be the radius of the external sphere; then $4\pi R^2_{i+1}-4\pi R^2_i$ determines the area of the part coloured in blue. Let R_c be the communication radius of a sensor; then $4\pi R^2_{i+1}-4\pi R^2_i/4\pi R^2_c$ permits to split up the blue part into areas of communication of a sensor. While simplifying the precedent operation, we get $(R^2_{i+1}-R^2_i)/R_c$ (**relation 1**)

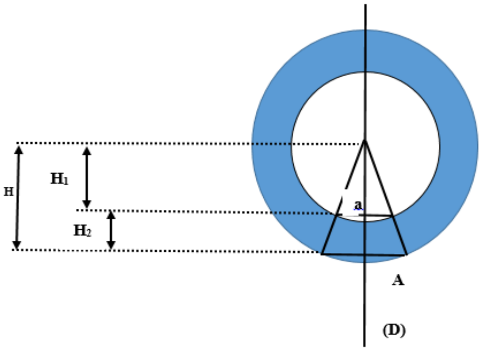


Figure 1. Determining the value of *a*

Let us consider that this area equals to the area of an isosceles trapezium where *a* is the small base, *A* is the highest base and H_2 is the height. α is the centre angle. The area of this trapezium is given by (A+a)*H_2/2. Let x=a/2. Then sin(α/2)= x/R_i; therefore a=2*R_i*sin(α/2). In the same way, A=2*R_{i+1}*sin(α/2).
H_2=H-H_1 = (R_{i+1}-R_i)*cos(α/2). Thus the area becomes
[(2*R_{i+1}*sin(α/2) + 2*R_i*sin(α/2))(R_{i+1}-R_i)*cos(α/2)]/2 = [2*sin(α/2)*cos(α/2)(R^2_{i+1}-R^2_i))]/2. However, 2*sin(α/2)*cos(α/2) = sin(α); the new area is given by: [sin(α)*(R^2_{i+1}-R^2_i)]/2 (**relation 2**).
While equalling relations 1 and 2, [sin(α)*(R^2_{i+1}-R^2_i)]/2 = (R^2_{i+1}-R^2_i)/R^2_c . Then we can conclude that sin(\α) = 2/R^2_c.

3.3.3 FORMATION OF VERTICAL SECTIONS

This formation is similar to the one of the horizontal section, always in a secure way and the angles are computed as indicated by the theorem 1.

3.3.4 DISCOVERING NEIGHBOURS ALGORITHM

The BS divides each cluster into *N* cells of radius *R* in order to determine the communication channels to re-use by different clusters according to the formula *D=R√(3N)* proposed in [16] where D is the re-use distance of a channel.

Thereafter, the sensors in each cluster broadcast their coordinates while respecting the CSMA/CA protocol [17] in order to avoid collisions. After a reception, each sensor compares these coordinates his own; if these are equal, he just adds the transmitter in his neighbour's list.

3.3.5 CLUSTER HEAD ELECTION IN EACH CLUSTER

Since the precedent steps consumed the same capacities in each sensor, the selected cluster head is the sensor having the smallest ID in each cluster. Thereafter, as soon as the energy of the CH will be less than a threshold, the CH is re-elected and the sensor having the highest energy will be chosen. As soon as the energy of all the sensors will be less than this threshold, a new threshold is computed using the average of the energy of all the sensors in a cluster and the re-election restarts.

3.3.6 NEW KEYS ESTABLISHMENT

At the end of the previous stage, the BS establishes a new key with each CH ($\mathbf{K_{(BS,CH)}}$), and the key $\mathbf{K_{(BS,CH*)}}$ used to authenticate communication between the BS and all the CHs. Then, in each cluster, the CH establishes the key $\mathbf{K_{(CH,M)}}$. Finally, the key K_{init} is deleted and communications are now secured using the keys $\mathbf{K_{(BS,CH)}}$, $\mathbf{K_{(BS,CH*)}}$ and $\mathbf{K_{(CH,M)}}$.

It is a key exchange in the manner of *Diffie and Hellman*, that means without communicating them directly. Each CH knows E(a,b,K) and *P*. Then each CH chooses an integer K_A and the BS chooses an integer K_B. Each CH sends to the BS the point K_AP of the elliptic curve, and the BS sends to all the CH the point K_BP. Each CH is therefore able to compute K_AK_BP; and this value is be the same for the BS. This point of the elliptic curve constitutes the secret key $\mathbf{K_{(BS,CH)}}$. Following the same principle, the keys $\mathbf{K_{(BS,CH*)}}$ and $\mathbf{K_{(CH,M)}}$ are established.

3.4 SECOND STAGE: ROUTING PHASE

After the first stage, the network is divided into l*m*n clusters in which each sensor knows his neighbours. Several virtual paths relying on the BS to each cluster are also created similarly to the virtual paths presented in [18]. All these paths meet at the BS thus creating a tree where the BS is the root, the nodes are the middle CHs and the leaves are the CH of the most distant clusters.
Here, the BS has an information to send to all the nodes located in the geocast region. This stage is being proceeded in two phases. The goal of the first phase is to discover all the nodes located in the geocast region. The second phase consists in sending information from the BS to these nodes. Note that the geocast region can be formed by the union of several clusters.

3.4.1 PHASE 1: DISCOVERY OF SENSORS IN THE GEOCAST REGION

The goal for the BS is to transmit data D in a geographic zone B. This phase consists in the discovery of nodes located in B. To save energy and reduce the execution time of this phase, let us specify that the time is divided into slots S^0, S^1... S^n. If the source wishes to send data to all nodes located in the geocast region, then at slot S^i, it spreads in the direction of the BS an item D, constituted of the message and the specifications of the geocast region. D = (REQUEST(Message, GeocastRegionCoordinates)). Having received the item, the BS sends a message M = SEARCH(GeocastRegionCoordinates, β, $\mathbf{K}_{(BS,CH^*)}$) containing the definition of the geocast region to all the CH using the key $\mathbf{K}_{(BS,CH^*)}$ in order to know if they have nodes situated in the geocast region specified in the message M. This message is accompanied with a binary variable β. Each CH has in its memory an array Δ of length 2. The first value of the array equals to 1 if some of its cluster's members are located in the zone B and 0 in the negative case. The second value of the array equals to 1 if the sons of the current CH have nodes in the zone B and 0 in the negative case. Each CH then sends the message to all its cluster's members by using the key $\mathbf{K}_{(CH,M)}$ and using the channel reservation technique [19]. Every node receiving the message checks its authenticity. It is informed about the zone B required and then is able to know if it is situated in this zone B or not (by using GPS). In the negative case, he makes nothing. In the positive case, he puts the binary variable β to 1, then sends a receipt acknowledgement to his CH. CHs having received at least a positive answer put the first value of the array Δ to 1 and forward to the BS an item (SEARCH(GeocastRegionCoordinates, $\mathbf{K}_{(BS,CH)}$, ID_{CH}, β = 1)). since data are forwarded to BS using the same principle than the one presented in [18] (by using virtual paths) and the technique of cyclic emission and reception [20], when the message arrives in a cluster, the CH makes an operation before forwarding the message. Indeed, when a CH receives the message coming from its son, it makes the operation "logical OR" on its variable β and the one coming from his son. If the result is 1, it puts the value 1 as the second value of the array and 0 if the result is 0. At the end of the slot S^i, if BS received at least one acknowledgement, then it knows where to send the D data to be transmitted.

3.4.2 PHASE 2: DATA DIFFUSION

For every sensor having answered the BS during time slot S^i, and being situated in zone B, the BS is able to send the information D to these sensors via their CH using the key $\mathbf{K}_{(BS,CH^*)}$.
Firstly, the BS broadcasts the information D in direction of the zone B. Each CH situated in the path linking the BS to the zone B checks its array Δ.

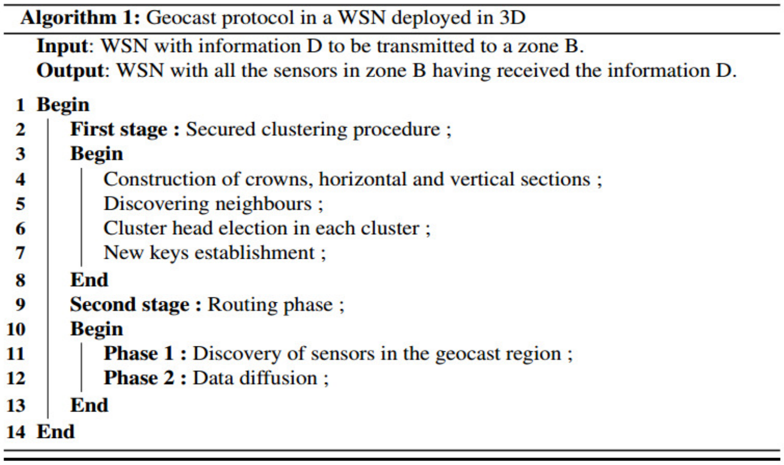
1- If the first and the second value of the array Δ are 0, then the CH does nothing.
2- If the first and the second value of the array Δ are 1, then the CH broadcasts the message D in its cluster using the key $\mathbf{K}_{(CH,M)}$ and forwards it to its son in the tree.

3- If the first value is 1 and the second is 0, then the CH broadcasts the message D in its cluster using the key $\mathbf{K}_{(CH,M)}$ and doesn't forwards it to its son.

4- If the first value is 0 and the second is 1, then the CH doesn't broadcast the message D in its cluster and just forward it to its son.

The information D is forwarded respecting this principle such as every cluster waiting for the information received this information. Then in each cluster, each sensor waiting for the information just copies it in its memory.

The pseudo-code of our protocol is given by the algorithm 1



```
Algorithm 1: Geocast protocol in a WSN deployed in 3D
  Input: WSN with information D to be transmitted to a zone B.
  Output: WSN with all the sensors in zone B having received the information D.
Begin
    First stage : Secured clustering procedure ;
    Begin
        Construction of crowns, horizontal and vertical sections ;
        Discovering neighbours ;
        Cluster head election in each cluster ;
        New keys establishment ;
    End
    Second stage : Routing phase ;
    Begin
        Phase 1 : Discovery of sensors in the geocast region ;
        Phase 2 : Data diffusion ;
    End
End
```

4. SECURITY ANALYSIS

Our protocol uses cryptographic keys to guarantee authentication and confidentiality on the exchanged messages. Indeed, while the clustering algorithm, all the stations use a unique key. However, if an attacker wants to know this key he has to solve the discrete logarithm problem which is a NP complete problem; therefore the time spent to determine the key is enough.

Thereafter, after the clustering stage, the initial key is deleted and new keys are established. Thus, the BS establishes a new key with each CH, a new key with all the CHs for messages in broadcast and each CH establishes a key with all his cluster's members.

This method of security avoids passive attacks whose goal is to read or update data circulating in the network such as *passive attacks, injection of messages, deterioration of message, Sybil attacks and message replication*.

5. SIMULATION RESULTS

The presented curves are the average of 100 experiments. We made the common assumption that two nodes are neighbours if and only if their Euclidean distance is less than 1 km. In our implementation, the MAC layer is managed in such a way that a node can only receive one message at a time with the number of items sets to 1000. To minimize the energy consumption, we used integers less than 255; thus, the maximal size of a key is 8 bits.

5.1 Evolution of Sensor's Energy

The energetic model we use is similar to the one in [21]. Let ET and ER be the energy used for the transmissions and the receptions of items in the network respectively. The energetic model of Heinzelman and al. is $E = ET+ER = a(e_t+e_{amp}*d^2) + n*e_r$. Each station initially has 1000J; 5J are used to transmit an item and 4j are used to receive an item. The curve in figure 2 presents the evolution of our nodes: normal nodes (in black) and CH nodes (in blue).

We can see that the clustering algorithm consume the same energy to all nodes; the variation of energy becomes visible while the routing stage.

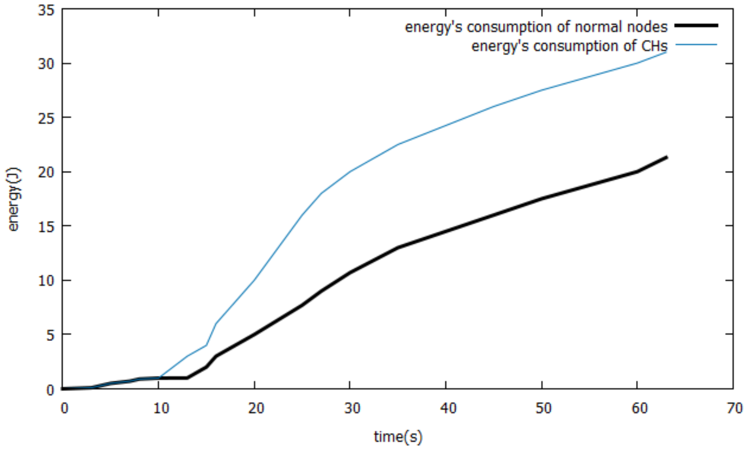


Figure 2. Evolution of sensor's energy

5.2 Network's lifetime

In order to put forward the efficiency of our protocol, we valued the lifetime of the network and we compared it with Myoupo and al. [11]. Figure 3 shows the results.

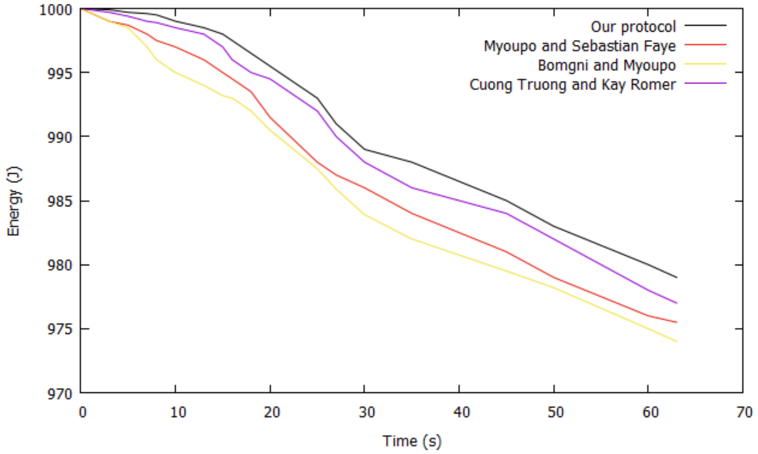


Figure 3. Network's lifetime

The protocol of Myoupo and al. [11] and the one of Bomgni and al. [13] consume more energy than our protocol because at the first stage they use the clustering algorithm of Sun and al. [2] and the one of Banerjee and al. [22] for the hierarchical clustering. The one of Cuong and al. [4] is more efficient than the protocols presented in [11] and [13]; but due to overhead during message exchanges, our protocol is better.

CONCLUSION

The solution presented in this paper is our secure approach to solving the problem of geocasting in a WSN deployed in space. The virtual structure on which our protocol is based allows a distributed network usage, and particularly effective use for control always provided by the BS. The security solution is a key management function based on elliptic curve cryptography (ECC) to generate symmetric keys and solve the key exchange problem between network sensor nodes after deployment. It avoids most attacks. In addition to combining the essential aspect of security, our protocol is fast and energy efficient.

Despite these encouraging results, several problems still remain. We plan to explore fault tolerant for geocast problem in dimension 3, which would ensure that normal stations will receive items in a finite time; another long-term perspective would be to create a safe environment for solving this problem taking into account that the base station is not the network centre and that it cannot reach all nodes. It would also be interesting to study the problem including some mobile nodes in the network.

REFERENCES

[1] M.David and H. Guyennet, (2008) “Etat de l'Art Sécurité dans les réseaux de capteurs SAR-SSI 3rd conference on Security of Network Architecture and Information Systems.

[2] S.Kun, P. Pai and N. Peng (2006) “Secure distributed cluster formation in wireless sensor networks”, 22nd annual Computer Security Application Conference, Las Vegas.

[3] W.Znaidi, (2010) “Quelques propositions de solutions pour la sécurité des réseaux de capteurs sans fil”, Institut national des sciences appliquées de Lyon.

[4] T.Cuong and R. Kay, (2010) “Practical 3D Geographic Routing for Wireless Sensor Networks”, Proceeding of the 8th ACM conference on Embedded Networked Sensor Systems.

[5] J.Sanchez, P. Ruiz, X. Liu and I. Stojmenovic, (2006) “Gmr: Geographic multicast routing for wireless sensor networks”, SECON.

[6] J.Sanchez, P. Ruiz, X. Liu and I. Stojmenovic, (2007) “Energy-efficient geographic multicast routing for sensor and actuator networks”, Computer Communication.

[7] M.Transier, H. Fler, J. Widmer, M. Mauve and W. Effelsberg, (2004) “Scalable position-based miulticast for mobile ad-hoc networks”, BroadWim.

[8] S.Wu and K. S. Candan, (2006) “Gmp: Distributed geographic multicast routing in wireless sensor networks”, ICDCS.

[9] Y.B.Ko and N. H. Vaidya, (1999) “Geocasting in mobile ad hoc networks: Location-based multicast algorithms”, WMCSA.

[10] A.Helmy and K. Seada, (2004) “Efficient geocasting with perfect delivery in wireless networks”, WNNC, IEEE.

[11] S.Faye and J. F. Myoupo, (2013) “Secure and energy-efficient geocast protocols for wireless sensor networks based on a hierarchical clustered structure”, International Journal of Network Security vol 15.

[12] N.Hadid and J. F. Myoupo, (2008) “Multi-geocast algorithms for wireless sparse or dense ad hoc sensor networks”, ICNS.

[13] A.B.Bomgni and J. F. Myoupo, (2010) “An energy-efficient clique-based geocast algorithm for dense sensor networks”, Communication And Network.

[14] C.-Y. Chang, C. -T. Chang and S. -C. Tu, (2003) “Obstacle-free geocasting protocols for single/multi-destination short message services in ad-hoc networks”, Wireless Network.

[15] V.K. Tchendji, J. F. Myoupo, P. L. Fotso and U. K. Zeukeng, (2017) “Virtual architecture and energy-efficient routing protocols for 3D wireless sensor networks”, International Journal of Wireless & Mobile Networks.

[16] B.J. Slimane, (2013) “Allocation conjointe des canaux de fréquence et des créneaux de temps et routage avec QdS dans les réseaux de capteurs sans fil denses et étendus”, Université de Lorraine.

[17] G.Pujolle, (2006) “Les réseaux”, EYROLLES.

[18] A.Wadaa, S. Olariu, L. Wilson and M. Eltoweissy, (2005) “Training a wireless sensor networks”, Mobile Networks and Applications vol 10.

[19] K.Nakano, S. Olariu and L. Schwing, (1999) “Broadcast-efficient protocols for mobile radio networks”, IEEE transactions on parallel and distributed systems vol 10.

[20] A.B. Bomgni, E. T. Fute, M. L. Foko and C. Tayou, (2016) “A tree-based distributed permutation routing protocol in multi hop wireless sensors network”, Wireless Sensor Network.

[21] W.R. Heinzelman, A. Chandrakasan and H. Balakrishnan, (2000) “Energy-Efficient communication protocol for wireless microsensor networks”, Proceedings of the 33th IEEE Hawii International Conference on systems.

[22] S.Banerjee and S. Khuller, (2001) “A clustering scheme for hierarchical control in multi-hop wireless networks”, Proceedings of the 20th IEEE International Conference on Computer Communications vol 3.

AUTHORS

Alain Bertrand Bomgni is a lecturer in the department of Mathematics and computer science of the University of Dschang (Dschang). He obtained the Ph.D from the University of Picardie Jules Verne (France) in 2013, his M.S. degree from the University of Yaounde I in 2006, and his B.S. degree from University of Dschang in 2002, all in computer science. His current research interests include parallel algoritms and architectures, distributed systems, wireless sensor network.

Elie FUTE T. is currently a lecturer in the Department of Mathematics and Computer science of the University of Dschang, and HOD of the Department of Computer Engineering at the Faculty of Engineering and Technology of the University of Buea. His field of study is computer science. He obtained his Ph.D degree from the university of **technology of Belfort-Montbeliard (France), in 2013, his M.S. degree from the** University oh Yaounde 1, and his B.S. degree from the University of Dschang. Modeling, Simulation, optimization, security and wireless sensor networks are his major research specialities.

Garrik Brel Jagho Mdemaya is a Phd student at the University of Dschang, Cameroon. He received his Master degree in computer science in 2016 from the University of Dschang. His current research interests include wireless communication and ad hoc networking.

Anastasie Kembouck Donfack is a Phd student at the University of Dschang, Cameroon. She received his Master degree in 2016 from the University of Dschang. Her current research include wireless communication and ad hoc networking.

Clémentin Tayou Djamegni received the DEA, Doctorat de troisième cycle and Doctorat d'Etat degrees in all computer science from the University of Yaounde I (Cameroon) in 1995, 1997 and 2005 respectively. In 1996, he joined the Faculty of sciences of the University of Dschang (Cameroon) where he is currently a professor and the head of the Department of Mathematics and computer science. Professor Djamegni help visiting research/faculty positions of IRISA, Faculté des sciences Jean Perrin and IRIT, all in France. His research interests include parallel algorithms, regular arrays, format concept analysis, distributed systems /algorithm, sensor networks, artificial intelligence, data mining, security and combinatorial problems