Secure and Energy-efficient Geocast Protocols for Wireless Sensor Networks Based on a Hierarchical Clustered Structure

Sébastien Faye and Jean Frédéric Myoupo
(Corresponding author: Jean Frédéric Myoupo)

Department of Computer Science, UFR Sciences, Université de Picardie-Jules Verne
33 rue Saint Leu, 80039 Amiens, France
(Email: jean-frederic.myoupo@u-picardie.fr)

(Received Apr. 20, 2012; revised and accepted July 5, 2012)

Abstract

This paper presents a secure and energy-efficient geocast protocol for wireless sensor network (WSN) based on a hierarchical clustered structure with data guarantee delivery from the base station (BS) all nodes placed in one or more geocast regions. Our protocol is composed of two major parts which are complementary and allow overall energy savings. First of all the hierarchical formation based on cliques and a concept of virtual architecture allows us to build a robust, fast and secure foundation for routing of information. Next geocast diffusion itself is simply reduced f a research phase in the network that is a step of sending data(s). Our protocol performs better in terms of less broadcast rounds overhead than the one in [33].

Keywords: Energy consumption, geocast, hierarchical clustering, security, wireless sensor networks

1 Introduction

The wireless sensor networks (WSN) are from the family of mobile ad-hoc (MANET), but have additional features and constraints: typically, they consist of a wide range of sensors with limited energy capacity. Each sensor is powered from a battery non-rechargeable and non-replaceable [3] and has a low capacity in terms of memory, calculation (CPU), and transmission range. Each sensor is able to harvest a set of data in a certain environment, and transmit it in multi-hop way to a base station (BS) or sink, which may act as instructor of the network. The use of such networks is widespread in many applications. For example we can mention the monitoring of forests, critical infrastructure, or the detection of biochemical agents and in the military industries. Some examples of work can be found through [1, 3, 15, 32].

In such a network, the security is a crucial point that we need to study and put forward. In fact, WSN have many constraints such as the communication medium, which is wireless: nowadays it is very easy to read, intercept and even modify the data transmitted, and to compromise an entire network. Let us add to these inconveniences the sensors application context, which are usually deployed in hostile environments. Thus there is a need to secure the protocols, in order to guarantee authentication, exchanges confidentiality [20, 30], data integrity and network availability. In the literature, several security protocols have been proposed. We can mention TinySec [17] or μTESLA [29] which ensures the authentication of the packets sent from a base station to the whole of nodes (broadcast or multicast), and that we use in this paper. Ultimately, a good security system should be able to avoid external attacks (coming from an attacker from outside the network) as well as the internal attacks (from an internal attacker of the network, by compromising a node).

The technology related to sensor networks advancing day by day, it is common to see WSN composed of several thousand units [16, 39]. In large networks, the sensors can be grouped into clusters based on their proximity to offer a better management and data transmissions in order to significantly increase the scalability, economy of energy, routing, and consequently the lifetime of the network (eg. [12, 24, 25, 36]). To maintain consistency, minimal hierarchy is created in each cluster, where the members agree on a chief: a cluster-head (CH for short), which is responsible for managing all members of its cluster and to carry out outwards operation.

In this paper we investigate a method of transmitting information, the geocasting (or geographical diffusion) that guarantees the data delivery to each sensor located at one or several specific locations of a network(geocast regions). To reach this goal we superpose two clustered architectures. First, the clustered WSN of Sun et al. [39] is used as the cluster of Level 1. A variant of the method for defining virtual architectures in [38] is developed here to produce clusters of Level 2 and higher. The structure provided by the use of clusters allows the use of different approach compared to what is generally suggested in the literature. The protocol that we present takes the main lines of [7], but is secure and able to avoid a majority of attacks [35]. Indeed, in addition to combining the essential aspect of

security, our protocol is energy-efficient. The multi cluster structure in which is based our protocol helps to minimize the broadcast overhead compared to the local structures approach with certain geocast regions (more constraining) proposed in [33] that yields huge broadcast rounds overhead.

The rest of this paper is organized as follows: in Section 2 we detail the state of art on geocast is presented with the concept of clustering and virtual architecture. Cluster formation and geocast protocols are presented in Section 3. In Section 4 study in detail the security provided by our solution. The energy consumption analysis of our solution is provided in Section 5. Some simulations are presented in Section 6. A conclusion ends the paper.

2 State of Art on Geocast

The most obvious approach to implement the geocasting is the use the flooding. BS sends a message to all its neighbors, which in turn relay the message to their own neighbors and so on, until all sensors in the geocast regions are reached and have knowledge of the message. Imielinski et al. [14] and Ko et al. [18] try to reduce the overall costs caused by flooding, which are very important. Besides the obvious aspect of flooding, many techniques have been developed in literature, for example around planar graphs. We can quote Face Routing [19] (which ensures the delivery of messages, but sometimes under constraint of a long transmission path), GFG [31] (Geographic-Forwarding-Geocast, which also ensures the delivery of the messages, but more effective with lower transmission costs), GFPG [34] (Geoagraphic-Forwarding-Perimeter-Geocast, use of a routing perimeter and guarantee delivery of packets even in not very dense networks), or VSF [22] (Virtual Surrounding Face). Also let us cite the paper [9], where the network is partitioned geographically: the suggested protocol makes it possible to create various paths according to the various possible geographical destinations. In the range of solutions described as purely secure, we can cite Palanisamy et al. protocol [27], based on an elaborate keys distribution mechanism, include the use of group keys to allow a member set to share information (received or emitted outside). Lastly, let us cite energy-efficient solutions which started to be studied in [12, 22, 40], where the various authors try to seek solutions to minimize energy consumption, an essential aspect in today's networks, and on which we present two literature approaches.

The first approach on which we wish to be delayed is the contribution of Y-C Shim [33], which presents a secure and energy-efficient solution of geocasting. The proposed protocol first is able to find a path to an access point. The first accessible sensor located in the geocast area. Then, starting from this node, the construction of a tree covering the whole area begins with the use of a broadcast technique limiting energy consumption. When done, established construction largely facilitates the sending and the reception of information in the geocast area. Security accompanying this structure is designed to prevent a majority of internal and external attacks: when a node sends a packet to another node, it checks if the receiving node processes the packet correctly and reports any unauthorized behavior detected. In addition, third "watch" nodes is used to solve additional problems. This protocol is effective in terms of detecting attacks however causes many transmissions (huge overhead) necessary to ensure a certain security and the use of tree structure. Also, the entire construction process described is repeated with each change of geocast area, which only increases the number of communications, and thus causes no significant loss of energy.

The second approach is that on which our protocol is based, namely the contribution of Bomgni et al. [8], which tackles the geocasting problem under uncommon way. In this paper, the authors propose a geocast protocol based on a hierarchical structure of clusters (initially cliques, for example [36], then using Banerjee et al. [4]). The use of clusters is ingenious because it allows us to carry out search mechanisms and efficient routing. Within this structure, a master sensor, say A, is obtained. When BS wishes to broadcast a message D to the area B, it sends a geocast region discovery message to node A. A launches a flooding on the network in order to discover the sensors that are in B. Finally the BS sends the message D after all acknowledgments received. This approach is quite original, but presents some disadvantages: on the one hand, the security is not assured, and the network can be an easy prey to external and internal attacks (example: the compromising of A would negate entire network); on the other hand, the network distribution is underdeveloped, and the fact that a single sensor is responsible of all the geocast diffusions can represent a major issue (fast exhaustion of energy, various overcosts, etc.).

2.1 Preliminaries on Clustering and Virtual Architecture

In order to better apprehend the next parts and in particular our formation protocol in 3.1 in this section details two fundamental aspects which we will use: first Sun et al. cliques clustering [39], then the concept of virtual architecture suggested by Wadaa et al. [38].

2.2 A Secure Clustering Protocol

As introduced earlier, nowadays it is common to find networks with many sensors, so there is a need to group those, using clusters. There are many works allowing their creation (example: [12, 24, 25, 36]) and are generally divided into two main families. On the one hand, leader-first protocols which first manage to elect a CH and to form clusters around (examples: LEACH [12], TEEN [24], APTEEN [25]). On the other hand cluster-first protocols which first form the clusters then elect a CH in each one. The retained solution is the latter and uses the protocol of Sun et al. [36]. Our choice referred to this protocol because it is secure (i.e. able to avoid a majority of internal and external attacks). And a protocol cluster-first is also better in the context of what we want to make: if changes were to

happen on the network at different CHs, we would just make a re-election. There should be no need to rebuild everything unlike first-leader protocol. Lastly, a major advantage of this protocol is that it is based on disjoint cliques formed by the representative graph of the WSN. This ensures us that inside each cluster each member can reach another member in only one hop, which reduces considerably the cost of certain communications. Figure 1(a) represents an example of network, while Figure 1(b) represents the application of Sun et al.'s protocol.

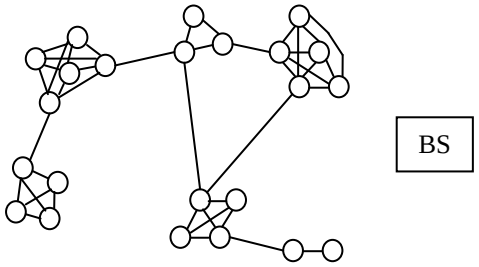

Figure 1(a): An example of WSN

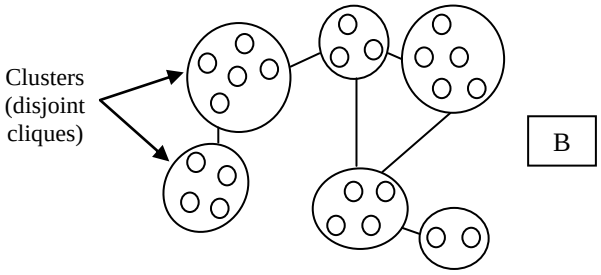

Figure 1(b): Sun *et al*. formation

2.3 Virtual Architecture

Consider a randomly gathered network of sensors around BS, which has the ability to transmit information to some powers (to the most distant sensor) and one-way (at certain angles). The concept of virtual architecture which matters to us is the one developed by Wadaa et al. [38]: the problem is that initially a node or set of nodes are not directly detectable by BS in space, no structure was clearly defined. The proposed solution therefore consists of a partition of the network into different zones (or areas) by BS. The latter has the possibility of disseminating information with more or less great range, this being used to create coronas; also, it has the possibility of disseminating information in certain directions, which is used by [40] in order to create various angular sectors. Zone (i, j) is the intersection of an angular Sector *j* and a Corona *i*. The sensors of the same area are therefore in the same geographical location and form a cluster. This is illustrated by Figure 2.

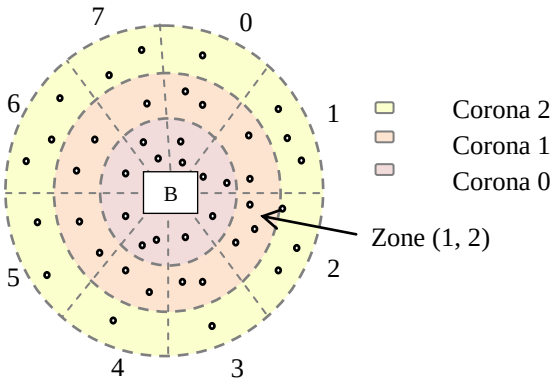

Figure 2: Virtual architecture

3 Secure Geocast Protocol

We first describe the model on which we rely, as well as the assumptions and conditions for the network initialization. The sub-section that follows is dedicated first to the secure structure formation. Next the geocast protocol itself follows.

3.1 Model, Assumptions and Security Issues

3.1.1 Notations

To clarify the continuation of our paper, we use the notations below. Some are not specified here but directly in the paper.

- [a-z]: Indicates a sensor.
- CH^N: Cluster-head of Level *N* (introduced in Section 3.1.2).
- ID_u: single identifying of 4 bytes corresponding to the Node *U*.
- $W^N\backslash\{w\}$: the whole of the nodes present in the cluster of Level *N* of Node *w* (without *w*).
- *WSN**: the whole of the sensors of the network.
- *a**: zero, one or more noted Nodes *a*.
- *a*,*b*: *a* concatenate to *b*.
- *B*: a geographical area.
- *D*: a message to be transmitted.
- *K{n/u}*: a one way keys chain of size *n+1* generated by Node *u*.
- *Ku,v*: a secret key shared between Nodes *u* and *v*.
- *Kbs,u*: a secret key shared between the base station and a Node *u*.
- $MAC_K(M)$: an authentication message of 8 bytes generated over M by using the key K.
- *H*: a one way hash function (uTESLA).

3.1.2 Model of Architecture

Our contribution is based on a layered clustering model. We yield a cascading Banerjee et al. protocol [4] over the clustered WSN (using [36]) with the goal to get many layers (or levels) of clustering. At the initial level, the nodes are partitioned into clusters called "of Level 1", and in each one of these clusters, a chief is being

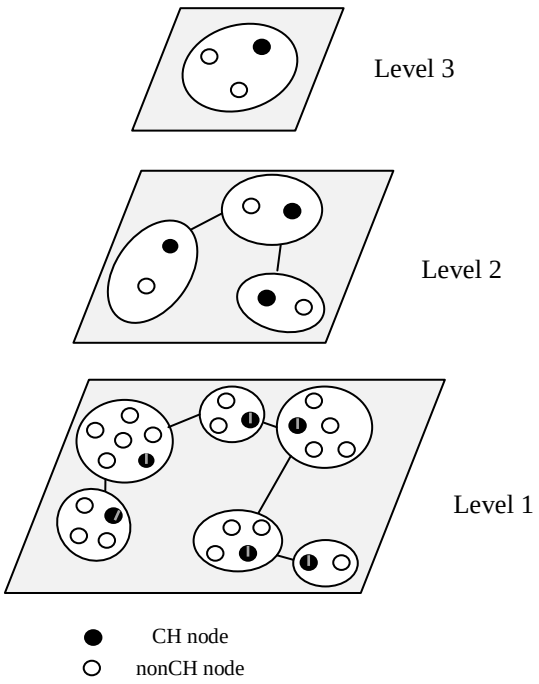

Figure 3: An example of our hierarchical formation

elected (a CH^1). The clusters of Level 1 are in their turn partitioned into clusters "of Level 2", and a chief would be elected for each cluster (a CH^2 elected among the CH^1s) and so till level N where the cluster head CH^{N+1} of each cluster of level N elected among the CH^Ns. This formation is illustrated in Figure 3.

If the advantageous distribution of the network is tempting, the challenge here is a security question: it is necessary for us to make sure that a geocasting is correctly carried out, without letting the network become an easy prey for the attackers and external threats.

3.1.3 Assumptions

(1). WSN is static, i.e. composed of immobile nodes once deployed. Optionally, adding and deleting nodes (for fault tolerance) is allowed, but considered rare.

(2). The base station (BS) is the only trusted entity in the network (it cannot be compromised), which has a strong energetic capacity than other nodes, and whose transmission range can cover the entire network. BS may also perform unidirectional transmissions (at certain angles).

(3). We suppose that each node shares a secret key with BS, which is charged before deployment. Also, each node is loaded with the necessary cryptographic material key establishment with its neighbors (using mechanisms as proposed in [5, 6, 8, 10, 37]).

(4). Each sensor is capable of locating itself in space using GPS, triangulation or a system of positioning for ad hoc networks (eg: APS [26]).

(5) We also consider the following properties: each node knows its neighbors at 1-hop and has a unique identifier. A message sent by a normal node can be received correctly by all its neighbors (1-hop). All the messages exchanged between two nodes are authenticated, thanks to the key shared between these nodes. Each node can generate a public key based on a signature (realist assumption compared to the literature: [11, 23]). The messages (broadcast) are authenticated thanks to a combination of signatures and uTESLA protocol. The signature is used for the nonrepudiation of the data. The protocol uTESLA is used for an effective authentication of broadcast. The clocks of the nodes are synchronized, as uTESLA requires it. The keys distributed by the various nodes and the base station are authenticated (use of uTESLA or a certificate in order to ensure the authenticity of a received key). Finally, let us recall that a WSN is always connected.

3.1.4 Security Issues

The existing attacks can be divided into two main types. On the one hand, the external attacks are generated by nodes being outside of the network and not having the cryptographic material necessary to understand the exchanged messages. Here a protection by using authentication techniques is generally enough to avoid the majority of the attacks, aside from jamming attacks tried on the entire network (as Sun et al. protocol indicates). On the other hand, the internal attacks aim to compromise nodes of the network. They can bypass the established protocol in order to obtain information, or arrive in our case to deflect information. The simplest case for an attacker to directly compromise a CH node is to provide incorrect results in a higher or lower level of the hierarchy, and cause a more consequent attack than by compromising traditional nodes.

Thus, the main objective of our protocol is to make safe the CH nodes, which are the first source attacks. Our protocol ensures that in the eventuality of compromising of CH nodes, transmission of information from BS to a given area is still performed without error. Details are given in Section 3. 3.

3.2 Heterogeneous Clusters Formation

We now present our cluster formation protocol which is necessary to obtain the structure which we have just described. The latter is divided into four main phases. First the initialization which is orchestrated by BS in order to set up on the one hand the cryptographic material necessary to the basic security of the network and on the other hand the various identifiers of the nodes. Next we use an existing and reliable protocol in order to build our first cluster level. This minimal structure is necessary to install an additional mechanism of keys. And we end up using a virtual architecture concept in order to form the next levels.

3.2.1 Phase 1: Initialization

This phase occurs before the network deployment. The base station first generates a chain of keys *K{n/bs}* needed to perform broadcasts to all authenticated sensors - in order to create our formation, or possibly for other operations: alerts, etc. -. It then charge each sensor u with a single identifying *IDu*, with a secret key *Kbs,u* shared with itself

in order to ensure future unicast communications (to guarantee confidentiality and authentication), and the first key *K{0/bs}* of its chain of key, in order to carry out broadcasts on the whole network (we use μTESLA use: to guarantee authentication). AT last, BS charges each node u with the cryptographic material key establishment with all its neighbors, for secure communications between pair of neighbor. Two neighboring nodes u and v has a shared key *Ku,v*.

3.2.2 Phase 2: First Level Cluster Construction

As indicated in Section 3.2.1., here we choose a secure cluster-first protocol in order to build in all serenity our first level and to ensure us of his solidity. This second phase is thus initially the application the Sun et al. protocol [36]. The latter uses the keys *Ku,v* set up between two nodes u and v, it also uses the authentication broadcast with μTESLA [29]: each node u generates – using its cryptographic material – a chain of keys *K{n/u}* and distributes the first key of the chain *K{0/u}* to its neighbors.

Let us notice that, this protocol does not take into account the typical example of the multiple identities (sybil) or wormhole attacks. However, these attacks can be detected by using known techniques of the literature as the work of Y. Hu et al. for sybil attack [28] and the work of B. Parno et al. for wormhole attack [13].

Once clusters created, the nodes inside each one agree on a chief and proceed to an election: we obtain a CH^1 in each cluster of Level 1. The structure obtained can be described such as Figure 3 suggests. Finally, each elected CH sends a message to BS containing the list of members of its cluster. The BS being informed by the network members, he is able to launch the following phase when it receives all CH acknowledgments.

3.2.3 Phase 3 (Recursive): Higher Levels Construction

The preceding phase enabled us to obtain a really healthy base for each cluster of Level 1. Now, as described in Section 3.2.2., we rely on a virtual architecture mechanism similar to [38] to partition our Level 1 clusters at higher levels. It's BS - only trusted entity in the network - which is in charge of this operation.

Initially, BS knows the network, and determines - according to the number of nodes and the will of partitioning fixed by the administrator - a range coefficient Cp (between 0.1 and 1 - 1 representative 100% of the distance separating BS of the most distant sensor in the network - this parameter can be given by successive BS broadcasts at the time of initialization - nondetailed) and an angular coefficient *Ca* (between 1° and 360°).

Everything then depends on the system administrator wishes: to make a lot of levels, we use a low *Ca* and *Cp*, to make a minimum we use a larger *Ca* and *Cp*. Other calculations related to virtual architecture are not detailed in this paper because are already fully the subjects of a study in [38]. BS thus is able to cut the network by making broadcasts to different ranges and angles, according to *Ca* and *Cp*, as it is suggested in Figure 4.

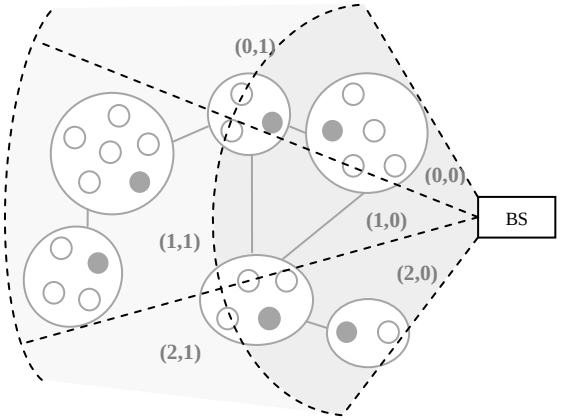

Figure 4. BS network cutting with Cp = 0.5 and Ca = 40°. Here, we take the second level formation case. Broadcast step.

Each zone defined by BS is indicated by a couple of integer: (angular number, corona number). The cluster generation process then is as follows for each level N (N > 1):

Step 1. BS performs a broadcast using the key K{n/bs} in order to communicate in an authenticated way the couple of integer to all nodes. BS thus successively broadcasts a message of the type (angle, corona) according to Ca and Cp and thus to various angles and coronas (eg on Figure 4).

For each zone (angle, corona) defined by BS according to Ca and Cp:

BS -> WSN : D,MAC$_{K\{j/bs\}}$(D),K{j/bs}*

With K{j/bs} the current key of the key chain K{n/bs}, D the integer couple to be sent and corresponding to a certain zone according to BS.

Each node u then receives the message. It first authenticates the - revealed - key *K{j/bs}* by using the previously stored key *K{j-1/bs}*: for that it uses the H irreversible hash function it holds, and checks the correspondence *K{j-1/bs} = H(K{j/bs})*. Once this first stage done, the node checks the authentication provided by MAC attached to the message and is able to upgrade its last known key. This is a simple application of the protocol uTESLA. Finally, a node is informed of the parameter (angle, corona) which is affected for him. Each node w ϵ CH^1 then communicates to all members of its Level 1 cluster the parameter that it holds, by using the key chain *K{j/w}* of *K{n/w}* for authentication (broadcast with uTESLA). The goal is to set in agreement all the members of each cluster of Level 1 (in case some members have a different setting).

$$w \rightarrow W^1 \backslash \{w\} : D, MAC_{K\{j/w\}}(D), K\{j/w\}$$

Step 2. They then read the parameter and upgrade their local value if there is a difference with the value broadcasted by BS, and return an acknowledgment

containing this end value to their CH^1, which is authenticated with *Ku,bs*.

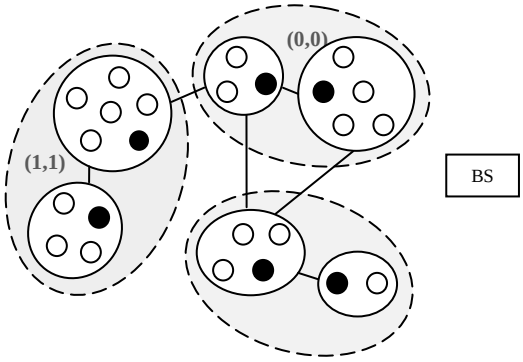

Figure 5: Level N formation (N > 1). Here, we take the case of Level 2 formation.

Step 3. Each CH^1 thus receives a group of answers that it cannot read or modify. Once all the responses received, it sends them all to BS, with the signature *Kch,bs*, by including *IDu* of members which have not responded.

Step 4. BS receives a message, authenticates it, and then checks one by one all the clusters nodes acknowledgments. If an inconsistency is noticed, or if it does not receive a message from a CH, it takes measures: re-election, banishment of nodes, or else.

Step 5. At this time, clusters of level N are implicitly formed: a cluster of level N is a set of clusters of level N-1, whose members have the same parameters (angle, corona) and are directly linked, as shown in Figure 5 (continuation of Figure 4).

Step 6. The continuation of the algorithm then consists of electing a CH^{N+1} among all the accessible CH^N between them without changing the parameter (angle, corona), like illustrates it Figure 6. Therefore a CH^{N+1} is also CH^N, CH^{N-1}, CH^{N-2},... CH^1. The cluster is considered to be formed. The cluster concept is a little bit abstract here, because a node belonging to a cluster of level N (N > 1) does not directly know all the other members, it has only knowledge of its CH^N and members of its Level 1 cluster. Here, we do not detail the election procedure itself, which depends on the parameters desired by the user (according to the supplied energy, of the identifier, etc.).

Step 7. Once the election made, each lately elected CH informs BS which starts again this entire phase for a higher level, by multiplying Cp and Ca by a factor i to fix. Cluster formation is complete when BS sees that there is nothing left but one CH for the Level N.

Cluster formation is completed and is not to be re-run. However it is possible that adjustment operations are performed internally, such as update operations: fault tolerance, adding nodes, or yet banishment mechanisms or re-election if a malicious node is detected.

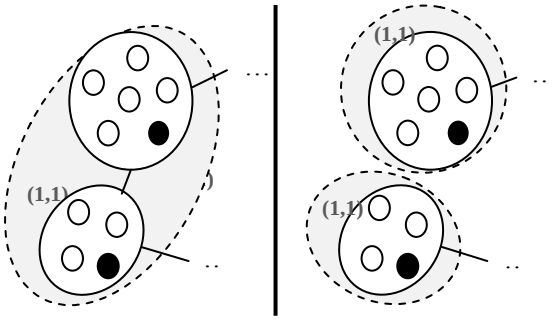

Figure 6: Need for accessibility for the clusters: the figure on the right is two clusters of Level 1 which is not interconnected. There has therefore creation of two clusters of Level 2.

3.2.4 Structure Maintenance

We suppose that the network on which our protocol proceeds is static (1) and always connected (5). However, it is common in such networks to add new sensors, or that because of energy constraints, links break or sensors disappear. Thus, it is necessary for us to manage this aspect and to ensure the good maintenance of the structure formed initially. To do so, the upgrade processes are simple to study, because they are based on an adaptation of the first level clusters. We can distinguish three cases:

Case 1: a new node is added. Here, two possible under-cases.

- If the new node can communicate with all existing members of a clique (Level 1 cluster), then it is simply added to that clique, and is responsible to be aware of CH^1, CH^2, ..., CH^N.
- If the new node communicates only with some nodes, without being able to reach all members of one clique, then the arriving node simply chooses the cluster with which it has the closest connection: it causes a cut of the latter into two Level 1 sub-clusters (according with our first phase, i.e. two cliques). Thus, one of the new clusters proceeds an election of CH^1, and the new node is informed by the higher levels CH.

Case 2: a node is removed from the network (malicious node, node without battery, etc.).

Case 3: a link is broken between two nodes (energy factor). Here, the second sub-case of our first case can be applied in order to solve the problem.

Thus, it is possible for us to adapt our network easily and to be able to manage a certain mobility, which remains in all the cases reduced, and which goes in agreement with the connection imposed in our Assumption (5).

3.3 The Geocast Protocol

The geocasting has two phases. Here, BS possesses information to be sent to nodes in geocast regions. The goal

of the first phase of our protocol is discovery of these nodes. The second phase consists of sending information since BS. This is illustrated through Figure 7 below.

3.3.1 Phase 1: Discovery of Sensors in the Geocast Regions

The objective for BS is to transmit a data D to a geographical area B. This phase consists in discovering the nodes located in B. In order to save energy and to limit the execution time of this phase, let us specify that time is divided into slots s^0, s^1,..., s^n. Our protocol follows the following steps:

Step 1. In slot s^i, BS first performs a broadcast using the key *K{n/bs}* in order to communicate in an authenticated way a small package representing the geographical zone B to the set of sensors in the network (uTESLA).

BS -> WSN : B,*$MAC_{K\{j/bs\}}$*(B),K{j/bs}*
With K{j/bs} the current key of the keys chain K{n/bs}, and B the zone to search.

Step 2. Each node u then receives the message and checks its authenticity. It is informed of the required zone B and then is able to know if it is located in it or not (Assumption (4)). In the negative case, it does nothing. In the positive case, it sends an acknowledgment to BS, containing B, authenticated using the shared key between BS and the node (*Kbs,u*).

u -> BS : B,$MAC_{Kbs,u}$*(B),Kbs,u*

Note that the routing from u to BS is done simply by going up the hierarchy determined by our structure.

Step 3. At the end of the slot s^i, if BS has received acknowledgments, then it knows where to send the data D to be transmitted.

3.3.2 Phase 2: Sending the Request

For each sensor u having responding to BS during the time slot s^i, and thus being located in B, BS is able to send directly to these sensors the information D, by authenticating it and protecting it with the Kbs,u key and during the time slot s^{i+1}. Note that the routing of BS to u uses the hierarchy determined by our structure. Figure 7 illustrates this situation.

3.3.3 Geocasting with Multiple Geocast Regions

On the basis of the protocol previously described, which only delivers an information to a single zone, it is possible for us to carry out parallel searches for multiple zones, by replacing the zone B by a concatenation of the various zones: "b1, b2,…, bn".

Theorem 3.1: *The above multi-stage clustering geocast algorithm guarantees the delivery to all nodes in the geocast region.*

Proof : Assume that there is at least one node in the geocast region that is not reached. Then this node has been disconnected from the network that is no more connected. Therefore it is not a sensor network. □

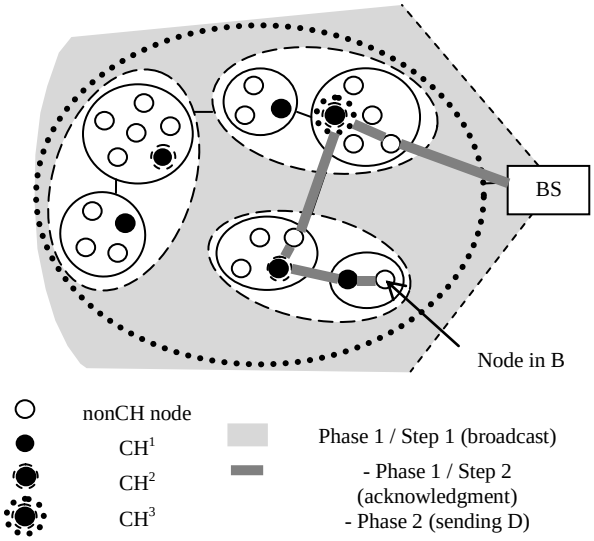

Figure 7: An application of our protocol

4 Security Analysis

We here study more in details the secure aspect of our protocol. We do not reconsider the formation protocol in which both the unfolding and the security seem clear to us, but directly on the geocast protocol, described in Section 3.3.

Concerning the first search phase for geocast regions, let us study the three stages sequentially. During the first stage, the protocol uTESLA [29] is used, which allows a transmission authenticated since BS. Each node receiving information is thus certain that it is an information item coming from BS, trusted entity of the network, and there is no mistake about this. At the end of the second phase, nodes u which wants to send an acknowledgment to BS uses the key *Kbs,u* to ensure the authenticity of the data to be returned. The routing as for him is done by simply going over the hierarchy of our structure, namely from a CH^1 to a CH^N. The authenticity of the package being guaranteed, it is impossible for a Node j located between *u* and *BS* to modify packets contents. In the same way if such a node does not wish to transmit information which is forwarded to it, the node u is able to detect the error after a certain time (in slots) because it has been informed that it will receive a message in Phase 2. AT the third step, BS is a trusted entity: there is no risk of attack.

The second phase consists in sending information to a node u located in B: BS uses *Kbs,u* key to encrypt and authenticate D to be transmitted. In the same way as for the second step of the previous phase, here the routing is from CH^N to a CH^1. Our protocol guarantees that if there is an attempt to modify, delete, or change the path of a data, this is detectable by BS, the only trusted entity in the network. A majority of the external attacks are thus avoided, and the compromising of CH nodes, however pillars of our

hierarchy, is also detectable. However, as described in Section 3.1.4, certain attacks are not managed by our protocol. It is a case, for example, of jamming attacks attempted on the whole network. For security and attacks on WSN the readers can find more details in [28, 29].

5 Energy Consumption Analysis

Here, we use a model adopted by many efficient contributions ([12, 40] for example).

$$E = ET + ER = N \times (e_t + e_{amp} \times d^n) + N \times e_r \quad (1)$$

Where *ET* and *ER* are the total energy used respectively in transmission on the network, and reception. In detail, *N* represents the number of nodes of the network, *D* the distance between the nodes, and *N* a parameter of energy attenuation ($2 \leq N \leq 4$). The energy used for the transmission is divided into energy for the radio transmission e_t and the amplifier e_{amp}. The energy used for the reception is represented by unit (for each node) by e_r.

***Strategy of locating the CH in the Central Area of the Cluster*:** Power consumption can thus be studied under various levels, starting with our hierarchical formation. On the one hand, power consumption is less inside each cluster of Level 1 (cliques), where each member has the possibility of communicating with another member in only one hop. Also, a CH^1 can directly broadcast to every member of its clique in one hop. Consequently, the energy required for the formation of clusters of Level 1 is less because based on cliques. This has a direct impact on the Equation (1). On the other hand, during the formation of higher levels clusters, it is the BS that supports most of the actions needed to this formation, which ensures lower energy consumption over all network, while providing some security. Logically, BS is an entity with more energy than other sensors. This poses no problem. As before, this has an impact on the Equation (1).

***Strategy of periodic hibernation*:** The study of energy consumption corresponding to our hierarchical formation being made, it remains for us to study the geocast protocol, which is composed of three major steps. First a broadcast made by BS on the entire network is done asking everyone to indicate whether it is in in the geocast region or not. Next a possible transmission of an acknowledgment in multi-hop of one or more sensors to BS follows. Finally sending in multi-hop the information from BS to these sensors is carried out while the sensors which are not concerned are asleep. While the basic broadcast is only a matter for BS and only implies the use of the parameter ER for each sensor, the two other steps consist of two routings: an upward one from one or more CH^1 to CH^N, and a descent one from CH^N to one or more CH^1. This routing is optimal in the sense that the path in which data items travel is simple, and does not consist in a flooding - even partial – of the network. Energy used is thus really minimized. Lastly, note that geocasting is performed using time slots, which can be used as sensors awakening slots. Definitely, for a geocasting in a zone B implying only one sensor, the energy consumption of a node is at least e_r, and to the maximum $2 \times (e_t + e_{amp} \times d^n) + 3 \times e_r$.

6 Simulation

In order to measure the effectiveness and to prove the flexibility of our formation protocol, we carried out some simulations which we describe through Figure 8 below.

We successively took a population of 50, 150 and 300 clusters of Level 1, as well as a whole of values for the coefficients *Ca* and *Cp*. For each possible case, we made 10 different simulations in order to evaluate an average location of the base station in the network, the distribution of different sensors, and the average number of clusters of Level 2 that are possible to construct for such features. The results are visible on the graph in Figure 8 and allow us to have a view of the flexibility provided by our formation: everything is really a function of *Ca* and *Cp* values, which are chosen depending on the application to achieve and on the density of information to be aggregated.

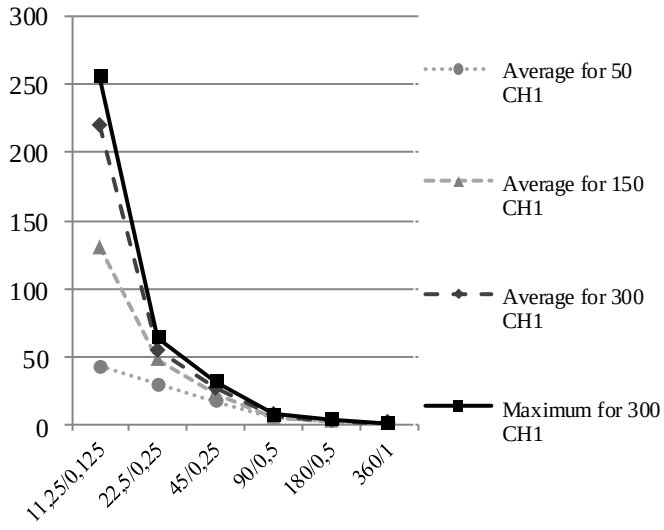

Figure 8: Number of Level 2 cluster depending on *Ca* and *Cp*

As we can see, the more we take a small value of *Ca* and *Cp*, the more the number of clusters of Level 2 rises, which enables us to have a certain control of the number of our clusters of Level 2. Concerning Level 1, very suitable simulations were carried out in Sun et al. paper [36]. Concerning the higher levels, the number of clusters depends on the multiplying coefficient on *Ca* and *Cp*, which we noted i. Let us take the case where *i* is equal to 2, and where $Ca = 180$ and $Cp = 0.5$ for Level 2. Then for Level 3 we have $Ca = 360$ and $CP = 1$. Thus Level 3 has only one cluster.

7 Conclusion

The solution suggested through this document is a secure approach making it possible to carry out in simple and fast manner geocasting in WSN. The hierarchical structure on

which our protocol is based allows a distributed use of the network, and especially efficient use, for a control always ensured by BS. It avoids a majority of attacks [36]. Indeed, in addition to combining the essential aspect of security, our protocol is energy-efficient and uses a global structure with the network to reduce overhead, instead of local structures with certain geocast regions (more constraining) that increase significantly the broadcast rounds overhead as it is the case for [33].

In future work, it would be interesting to study the problem by including certain nodes mobility in the network. Although fault tolerance and the addition of nodes are discussed here, the dynamics of the network are still very limited.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] J. Agre and L. Clare, "An integrated architecture for cooperative sensing networks," *IEEE Computer*, vol. 33, no. 5, pp. 106-108, 2000.

[2] J. N. AI-Karaki, R. UI-Mustafa, and A. E. Kamal, "Data aggregation in wireless sensor networks - exact and approximate algorithms," *Workshop on High Performance Switching and Routing*, pp. 241- 245, Apr. 19-21, 2004.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Computer Networks*, vol. 38, pp. 393-422, 2002.

[4] S. Banerjee and S. Khuller, "A clustering scheme for hierarchical control in multihop wireless networks," in *Proceedings of the 20th IEEE IINFOCOM*, vol. 2, pp. 1028-1037, 2001.

[5] R. Blom, "An optimal class of symmetric key generation," *Advances in Cryptography- Eurocrypt' 84*, LNCS 209, pp. 335-338, Springer-Verlag, Berlin, 1984.

[6] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly secure key distribution for dynamic conferences," in *Proceedings of the 12th Annual International Cryptology Conferenc*e, LNCS 17, pp. 471-486, 1992.

[7] A. B. Bomgni and J. F. Myoupo, "An energy-efficient clique-based geocast algorithm for dense sensor networks," *Communications and Network*, vol. 2, pp. 125-133, 2010.

[8] H. Chan, A. Perrig, and D. Song, "Random key predistibution schemes for sensor networks," *IEEE Symposium on Security and Privacy*, pp. 197-213, Okland California USA, 2003.

[9] C. Y. Chang, C. T. Chang, and S. C. Tu, "Obstacle free geocasting protocols for single/multi- destination short message services in ad hoc networks," *Wireless Networks*, vol. 9, no. 2, pp. 143-155, 2003.

[10] T. Dimitriou and I. Krontiris, "A localized, distributed protocol for secure information exchange in sensor networks," in *Proceedings of the 19th IEEE Internationa Parallel and Distributed Processing Symposium*, pp. 240a, 2005.

[11] N. Gura, A. Patel, and A. Wander, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in *Proceedings of the 2004 Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, pp. 119-132, 2004.

[12] W. R. Heinzelman, A. Chandrakasan, and H. Balak-rishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33th IEEE Hawii International Conference on Systems*, pp. 3005-3014, 2000.

[13] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks," in *INFOCOM*, pp. 1976-1986, April 2003.

[14] T. Imielinski and J. Navas, GPS-Based Addressing and Routing, RFC 2009 Computer Science, Rutgers Univer-sity Press, Rutgers, Mar. 1996.

[15] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," in *Proceedings of MOBICOM' 00*, pp. 56-67, 2000.

[16] J. M Kahn, R. H Katz, and K. S. J. Pister, "Mobile networking for smart dust," in proceedings of MOBICOM' 99, pp. 17-19, 1999.

[17] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," in P*roceedings of the 2nd international conference on Embedded networked sensor systems*, vol. V, pp. 162-175, 2004.

[18] Y. B. Ko and N. H. Vaidya, "Flooding-based geocasting protocols for mobile ad hoc networks," *MONET*, vol. 7, no. 6, pp. 471-480, 2002.

[19] E. Kranakis, H. Singh, and J. Urrutia, "Compass routing on geometric networks," *Proceedings of 11th Canadian Conference on Computational Geometry*, pp. 51-54, Vancouver, Aug. 1999.

[20] C. Li, Z. Wang, and C. Yang, "Secure routing for wireless mesh networks," *International Journal of Network Security*, vol. 13, No. 2, pp. 109-120, 2011

[21] J. Lian, K. Naik, Y. Liu and L. Chen, "Virtual surround-ing face geocasting with guaranteed message delivery for sensor networks," in *Proceedings of the 14th IEEE International Conference on Network Protocols*, pp. 198-207, 2006.

[22] J. S. Liu and C. H. R. Lin, "Energy-efficient clustering protocol in wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 3, pp. 371-388, May 2005.

[23] D. J. Malan, M.Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography,"*SECON*, pp. 71-80, Oct. 2004.

[24] A. Manjeshwar and D. Agrawal, "TEEN: A protocol for enhanced efficiency in WSN," in *Proceedings of*

the 15th International Parallel & Distributed Processing Symposium, pp. 2009-2015, Apr. 23-27, 2001.

[25] A. Manjeshwar and D. Agrawal, "APTEEN: A hybrid protocol for efficient routing and a comprehensive information retrieval in WSN," in *Proceedings of the International Parallel and Distributed Processing Symposium*, pp. 195-202, Apr. 15-19, 2002.

[26] D. Niculescu and B. Nath, "Ad hoc positioning system (APS)," in *Proceedings of IEEE Global Tele-communications Conference*, pp. 2926-2931, San Antonio, 2001.

[27] V. Palanisamy and P. Annadurai, "Secure geocast in ad hoc network using multicasting key distribution scheme (SGAMKDS)," *International Association of Computer Science and Information Technology - Spring Conference*, pp. 190-194, 2009.

[28] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," *IEEE Symposium on Security and Privacy*, pp. 49-63, 2005.

[29] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "Spins: Security protocols for sensor networks," in *Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, pp. 189-199, 2001.

[30] I. A. Saroit, S. F. El-Zoghdy, and M. Matar, "A scalable and distributed security protocol for multicast communications," I*nternational Journal of Network Security*, vol. 12, no. 2, pp. 61-74, 2011.

[31] K. Seada and A. Helmy, "Efficient geocasting with per-fect delivery in wireless networks," *IEEE Wireless Communications and Networking Conference*, pp. 2551-2556, 2004.

[32] C. C. Shen, C. Srisathapornphat, and C. Jaikaeo, "Sensor information networking architecture and applications," *IEEE Personal Communications*, pp. 52-59, 2000.

[33] Y. C. Shim, "Secure and energy efficient geocast protocol for sensor networks with misbehaving nodes," I*nternational Journal of Communications*, vol. 2, pp. 222-229, 2009.

[34] I. Stojmenovic, "Geocasting with guaranteed delivery in sensor networks," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 29-37, Dec. 2004.

[35] E. Schoch, F. Kargl, T. Leinmuller, and M. Weber, "Vulnerabilities of Geocast Message Distribution," *2nd IEEE Workshop on Automotive Networking and Applications (AutoNet 2007)*, pp. 1-8, Washington, DC, USA, 2007.

[36] K. Sun, P. Peng, P. Ning and C. Wang, "Secure distributed cluster formation in wireless sensor networks," *22nd Annual Computer Security App-lications Conference*, pp. 131-140. 2006.

[37] S. F. Tzeng, C. C. Lee, and T. C. Lin, "a novel key management scheme for dynamic access control in a hierarchy," *International Journal of Network Security*, vol. 12, no. 3, pp. 178-180, 2011.

[38] A. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy, and K. Jones, "Training a wireless sensor network," *Mobile Networks and Applications*, vol.10, pp.151-168, 2005.

[39] B. Warneke, M. Last, B. Leibowitz, and K. Pister, "SmartDust: communicating with a cubic-millimeter computer," *IEEE Computers*, vol. 34, pp. 44-51, 2001.

[40] D. Wei, S. Kaplan, and H. A. Chan, "Energy efficient clustering algorithms for wireless, sensor networks," in *Proceedings of IEEE Conference on Communications*, pp. 236-240, Beijing, 2008.

Jean Frédéric Myoupo is Professor of Computer Science in the University of Picardie-Jules Verne, Amiens, France where he heads the parallel and Mobile computing group. He has been Dean of this Faculty from 1999 to 2002. He received his Ph.D in applied mathematics from the Paul Sabatier University of Toulouse in 1983. He held many positions in mathematics and computer science departments such as lecturer or associate professor in different universities: the university of Sherbrooke, Québec from 193 to 1985, the university of Yaounde, Cameroon from 1985 to 1990; the university of Paris 11, Orsay, France from 1990 to 1993 and the university of Rouen, France from 1993-1994. Professor Myoupo has served as member of program committee of international conferences as PDPTA, CIC, OPODIS, - IPDPS workshops, HPCS. AP2PS, WINSYS, ICNS, ICWN, IEEE-RIVF, IEEE ISSPIT, ISCA-PDCS. Dr Myoupo is an Associate Editor of "*ISCA International Journal on Computers and their Applications"* and a Member of the editorial board of "*Studia Informatica Universalis, Communication and Networks and* ISRN Sensor Networks ''. His current research interests include parallel algorithms and architectures, Interconnection Networks, Wireless communication and security, and mobile computing.

Sébastien Faye is a Ph.D student. He obtained the Master degree in computer on June 2011 from the university of Picardie Jules Verne. His current research interests include wireless communications and wireless network security.