Security Study of the Controlled Greedy Sleep (CGS) algorithm

Alexandre Pocquet*, Bernard Cousin†, Miklos Molnar‡ , and Patrice Parraud§
*IRISA, MACCLIA laboratory of Military Special School of Saint-Cyr, France
†IRISA, University of Rennes I, France
‡IRISA, INSA Rennes, France
§INSA Rennes, MACCLIA laboratory of Military Special School of Saint-Cyr, France

***Abstract*—This paper deals with the CGS' algorithm security. CGS is an algorithm that attempt to increase the lifetime of fixed overdosed wireless sensors networks that have to provide the K-coverage of an area. CGS is based on periodic messages exchanges between sensors in order to determine which of them are the most critical and are eventually allowed to go to sleep for a period of time. A after a presentation of the CGS' objectives and course. We bring to the fore CGS' vulnerabilities due to attacks on messages by intruder sensors to decrease the quality of service and/or the lifetime of the network. Finally, we conclude on what is the main security need to avoid such attacks and propose a cryptographic scheme to improve the CGS' security.**

I. Introduction

This part presents, the algorithm CGS' objectives, its course, its different messages, definitions and some working hypothesis in the context of the k-coverage of a an area by a static overdosed wireless sensors network [6].

A. Presentation of the CGS algorithm

1) Objectives and course of the CGS algorithm: The CGS algorithm [1] attempts to maximize the lifetime of a sensors network which is a k-coverage provider of an area. Indeed, sensors networks are limited by their number of sensors, their lack of autonomy, their low computational power, their measure and communication radius (Rm and Rc) . CGS is based on the time division per period and the space division of the area per region (r). The regions are covered by active sensors that have been placed from them at a distance less or equal to their measure radius.

The objectives are the following:

- The better quality of service on the area : do the periodic selection into the set of sensor of (a new) subset of sensors that must stay temporarily active to provide the k-coverage of all the regions.
- Decrease and share out the k-coverage cost: limit the number of active sensors during each period and taking into account the sensors local situations and energy levels for the selection of the subset. Minimize the messages sending

.

And to reach these objectives, CGS makes sensors detect their neighbor sensors, compute Drowsiness factor (Ds) and communicate the associated Decision Time Delay (DTD) that are two priority metrics used to select the subset of active sensors.

There are the main steps of the CGS' algorithm:

- Run the network for a period T, the coverage is provided by the active (awake) sensors.
- All sensors in the network wake up at the end of each period.
- Nodes with remaining energy level high enough for at least one more period of operation broadcast local Hello messages containing their coordinates. Based on received Hello messages each sensor builds up its local set of alive neighbor sensors (S) and store their coordinates informations.
- Based on the received Hello messages, each sensor compute its Ds.
- Based on Ds each sensor selects a DTD with the following rules: a small drowsiness means a large DTD and a large Ds means small a DTD. These delays provide priorities when sensors announce their Awake Messages.
- Each sensor broadcasts its DTD message and starts collecting other sensor DTD and Awake Messages (AM). From the received DTD messages each sensor builds a Delay List (DL), and from the received AM, it builds a List of Awake Neighbors (LAN).
- After DTD elapsed each sensor makes a decision based upon LAN and DL:
  - if all regions (in the area) that it can cover, can be k-covered using only sensors present in LAN and/or sensors in DL which have a greater DTD the sensor goes to sleep.
  - otherwise the sensor stay awake and broadcast an AM to inform its neighbor sensors about its decision.

The drowsiness factor of a node with remaining energy E_s and which can cover an area R is defined as follows:

$$Ds = \begin{cases} \frac{1}{E_s^\alpha} \sum_{\forall r \in R} \text{if } \phi_r > 0, \forall r \\ -1 \text{ otherwise} \end{cases}$$

and α is a positive constant (e.g. $\alpha = 2$), and ϕ_r is the coverage ratio of region r defined as follows:

$$\phi_r = \begin{cases} \frac{1}{c_r - k} \text{ if } c_r > k \\ -1 \text{ otherwise} \end{cases}$$

where c_r is the number of linked sensors for the region r. The coverage ratio is positive if only the region is over-covered, i.e. more than k sensors that could cover region r. It is negative if region r is not over-covered: in this case the operation of all sensors possibly covering r is essential.

2) Definitions and hypothesis for the study:

- Quality of service [1]: ratio between number of regions leather or equal than k-covered and the number of regions less than k-covered.
- Legitimate sensor: sensor that has been as normally placed on the area and that attempts to make its contribution to the k-coverage.
- Intruder sensor: sensor which is not legitimate and for which the objectives are to decrease the quality of service and/or increase its cost.
- Corrupt sensor: sensor that has been as normally placed on the area but that has the same objectives as an intruder sensor.
- Measure radius: maximum distance from a region to a sensor to be covered by it.
- Communication radius: maximum distance between two sensor to communicate.
- Neighbor sensors: sensors which can communicate together.
- Linked sensors: sensors which can cover one or more same regions. That mean there are at a distance from each other less or equal than the twice measure radius.

Working hypothesis for the study:

- There are no corrupt sensors.
- The communication radius is greater than the twice of the measure radius. So linked sensors are also neighbor sensors.
- All legitimate sensors have the same measure radius, the same communication radius and energy level.
- Legitimate sensors are placed an area within a grid.

Despite of these optimistic hypothesis, the next part demonstrates that there are several specific attacks led by just a few intruder sensors that would be injurious to the quality of service and/or and the cost of the k-coverage.

II. Attacks on CGS algorithm by intruder sensors

This section presents some specific attacks executed by intruder sensors by using fake messages during the different steps of the algorithm. Its show that these attacks which can be mixed, mainly use two strategies with their own objectives:

- Simulate in an area the presence of extra sensors which are linked with the legitimate sensor which cover this area. The goal is to encourage legitimate sensors to sleep in order to decrease the quality of service.
- Introduce confusion on messages and its sender (legitimate sensor) by sending different versions of the message. The purpose is to discredit the sender legitimate sensor on their linked sensors point of view to force them to ignore the discredited legitimate sensor coverage capacity. The result could be a bad selection of the awake sensors subset and increasing k-coverage cost.

At the end of this part we present the increase of influences and difficulties for the detection of the exhibited attacks in the case of they are knowingly performed and mixed during all periods and steps of the algorithm.

This is the network configuration: legitimate sensors are placed on a grid such as distance between adjacent sensors is $10m$, measure and communication radius are respectively $15m$ and approximately $40m$, energy level of all is set to $1unit$ and the required coverage is $k = 3$, and due to the small area size all legitimate sensors are linked.

A. Attacks on Hello messages

1) Simulation of extra linked sensors by sending fake Hello Messages: The intruder sensors (black disk on figure 1) send to neighbor legitimate sensors (black rings with a number in the center on figure 1) Hello messages about extra linked sensors. So that legitimate neighbor sensors add these extra linked sensors to their set of alive sensors neighbors. The figure 1 shows two configurations with a different area to cover (space into the rectangular in shape black outline).

In case *a* intruder sensors simulates two extra sensors at their coordinate so that legitimate sensors Drowsiness Factor values decrease (fake values are on the left upper side and real value on the right upper side of the sensors)s. If we compare the real and fake Drowsiness Factor values, we notice that the hierarchy of the Drowsiness factor has changed. Indeed, sensors 0 and 3 have after attack the higher Drowsiness Factor values (0.43) instead of sensors 1 and 4 (0.40 value after attack) and probably sensors 0 or 3 will be priority to go to sleep.

b situation is one of the worst case. We have voluntarily add new regions by stretching the area on the right side of sensor 2 and 5 to create a situation where uneventfully sensors 0 or 3 only may go to sleep (with a Ds value of 0.66). Due to the others sensors Df values -1 since some of these new regions (on the upper and lower right side) are 3-covered at most. This attack by simulation of presence of only one extra linked sensor makes believe the possible (k+1)-coverage of the new regions. This attack place sensor

1 and 4 on the top of the list to go to sleep and so threats the quality of service.

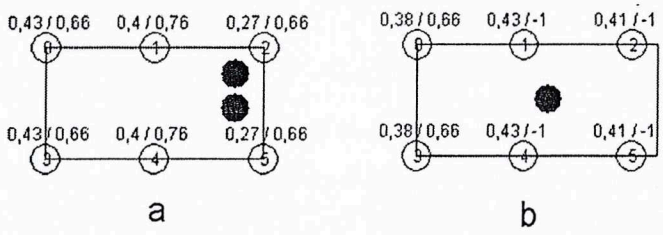

Fig. 1. Attacks by simulation of extra linked sensors presences in order to modify the Drowsiness Factor values.

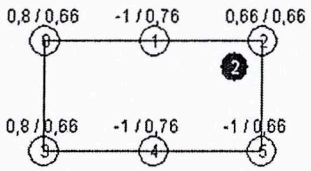

Fig. 2. Attacks by sending several versions of a Hello Message with different coordinates so that the sender legitimate sensors coverage capacities are ignored.

2) Attacks by sending other versions of a Hello Message with different coordinates: As in figure 2 an intruder sensor send an other version of Hello message send by a legitimate sensor (legitimate sensor 2) with different coordinates. Thus receiver sensors can't be sure of the coordinates of the sensor attacked (see the true and the virtual sensor 2 on figure 2) and could ignore its presence if they don't its true coordinates. As a consequence in figure 2, sensors 1,4 and 5 have after attacks a new Ds value of -1 which forbids them to go to sleep and could increase the cost of the k-coverage.

We notes that these two attacks have not the same objectives but are twice more efficient if they start from the first period. In fact, the first attack by simulation of presence may be easily detected if the intruder sensor makes extra linked sensors appear after the application. Except of course if the intruder sensor extends virtually the life of a now-dead legitimate sensor at the same place. The second attack by sending an other version is by definition detectable but it needs to be started from the first period to prevent other sensor from knowing the true coordinates of the attacked sensor and discard fake messages.

B. Attacks on Decision Time Delay messages

1) Simulation of extra sensors presence by sending fake DTD messages: We distinguish two cases which mainly aim the decrease of the quality of service.

- Simulation of extra sensors presence with low DTD value: if legitimate sensors receive extra linked sensors DTD messages with higher DTD values, then the intruder sensors will be expected to convey its decision at first of the next step. That could be interesting to the attackers to simulate on the next step the early awake of extra sensors.
- Simulation of extra sensors presence with high DTD value: if legitimate sensors receive extra linked sensors DTD messages with lower DTD values then the intruder sensor will be expected to convey its decision at last on the next steps. This case is also dangerous because attackers may make believe the presence of extra sensor which could sacrifice itself to provide the coverage if the others legitimate sensors (with lower DTD values) need to sleep.

2) Attacks by sending other versions of a DTD message with different DTD values and/or coordinates: If intruder sensor send others versions of a DTD message legitimate sensor message with different but coherent DTD values. Then it will be difficult for neighbor sensors to select the good message with the real DTD value.
Once again this attack is very interesting in case of organisation of an attack on the next step. **We think this attack is the easier to do because there are possible during any period and almost without any preparation.** The attack about different coordinates is also possible but needs before to be credible others attacks on Hello messages coordinates. Otherwise neighbor sensors may compare coordinates exchanged during antecedent periods and steps.

C. Attacks on Awake Messages

Attacks on Awake Messages (AM) are special because legitimate sensors only send Awake Message if they stay active during the period. So an intruder sensor can't simulate the sleeping of an active legitimate sensor which sent its AM. It's not possible to discredit active legitimate sensor AM with different values since the Awake information is just a flag unlike the DTD' metric. However an attacker has the possibility to send different version of an Awake Message with different coordinates if such attacks were done on previous messages. The best possibility for an intruder sensor to attack AM is to simulate the awake of a sleeping sensor by sending a fake AM before its DTD expiration. This attack is easy to succeed in because it's could be only detected by the targeted legitimate sensor which can't prove it's sleeping.

D. Combining of attacks on Hello, DTD, and Awake messages

The combining of the previously shown attacks from the start of the k-coverage application and on each period may increase the efficiency intruder sensors interventions. So an intruder sensor could be able to simulate without suspicious the presence and k-coverage participation of a few extra linked sensors (like in Sybil attack, see chapter 9 of [5] and chapter 30 of [4]) during all the application periods. It's an important menace to the quality of service. This intruder can also discredit all the time a few legitimate sensors to incite

their linked sensors to stay continually alive (increase the k-coverage cost) and at the end make them die prematurely (reduce quality of service).

III. Conclusion

Most of attacks we have shown aim to discredit legitimate sensors messages information or simulate extra linked sensor presence and activity. As means and consequences are different, necessarily we have to study separately ad-libbed attacks and organized ones. But all these kind of attacks could be very dangerous due to the fact that an intruder sensor can attacks several neighbor legitimate sensors at the same time. So we could imagine how prejudicial it could be if these attacks are combined by each member of an intruder sensors coalition (like in Byzantine attack, see chapter 9 of [5] and chapter 30 of [4]).

These attacks reveals a capital authentication and/or integrity need for securing the algorithm. We propose in taking account the poor computational power sensors capacities the uses of some cryptographic primitives like Message Authentication Code (see chapter 9 of [3]) using hash function (see chapter 7 of [2]) and a secret key shared between legitimate sensors. It could increase a lot the algorithm protection against attacks if we consider that there are no corrupt sensors.

References

[1] G.Simon and M.Molnar and L.Gnczy and B.Cousin, *Dependable k-coverage algoritms for sensor networks*, Technology Conference - IMTC 2007.

[2] A.Poli and P.Guillot, *Algbre et protection de l'information*, computer science collection, Lavoisier.

[3] A.J.Menezes and P.C.Van Oorschot and S.A.Vanstone, *Handbook of Applied Cryptography*, Computers Sciences Applied Mathematics Engineering, CRC Press, 1997.

[4] C.Siva Ram Murthy and B.S.Manoj and *Ad Hoc Wireless Networks Architectures and Protocols*, Pentice Hall Communications Engineering and Emerging Technologies, Pearson Education, 2004, Fourth edition.

[5] M.Ilyas, *The Handbook of Ad-Hoc Wireless Networks*, Electrical Engineering Handbook, CRC PRESS, 2003.

[6] S.Kumar, T.H.Lai and J.Balogh and *On k-coverage in a mostly sleeping sensor network*, Proceedings of the 10th Annual International Conference on Mobile Computing and Networking MobiCom ', 2004.