Journal of Yasar University
http://joy.yasar.edu.tr

QUALITY OF SERVICE AND SECURITY CONTROL FOR CLUSTER-BASED WIRELESS SENSOR NETWORKS

Emrah TOMUR*

ABSTRACT

In this study, we investigate security and quality of service (QoS) issues in cluster-based wireless sensor networks (WSN). Our QoS definition consists of four attributes, which are spatial resolution, coverage, network lifetime and packet collisions. And, the security scope of our study is limited by message integrity and authentication. We present a novel control strategy to maintain desired QoS and security levels during the entire operation of a cluster-based sensor network. Compared to our previous work [1], the proposed method provides much better results for three of the four service quality attributes. This study also presents a method for determining the best tradeoff between security and spatial resolution for cases where network capacity is not sufficient to support required security and resolution levels. This method is based on a heuristic algorithm that we developed to solve an optimization problem.

Keywords: Sensor networks, security, QoS, spatial resolution, coverage.

1 INTRODUCTION

Wireless sensor networks provide efficient and reliable means for the observation of some physical phenomena which are otherwise very difficult, if not impossible, to observe, and initiation of right actions based on collective information received from sensor nodes. This feature of WSN has significant impact on several military and civil applications such as disaster management, field surveillance and environmental monitoring.

* *Department of Information Systems, Middle East Technical University, Ankara, Turkey.*
E-mail: emrah.tomur@gmail.com

In order to enhance existing applications and explore new potential WSN applications, there has been considerable amount of research conducted on sensor networks. Due to strict energy limitations of sensor nodes and their deployment in large numbers, most of the research effort on WSN focused on scalable and energy-aware communication protocols which aim to maximize network lifetime [2][3]. As medium access is a major consumer of sensor energy, power-efficient medium access control (MAC) mechanisms are also explored in different studies [4]. The common feature of these research studies is that they address the communication problems of WSN applications which require conventional data communications which is energy-efficient. Nonetheless, there has not been much research regarding the quality of service issues in wireless sensor networks.

One of the recent works that introduce QoS concept for sensor networks is [5] where authors define sensor network QoS as the *optimum number of sensors sending information towards information-collecting sinks, typically base stations.* This definition equates service quality to *spatial resolution* referring to the number of sensors which are active in sending data towards the information sinks so that necessary information required for system functionality can be extracted from collected raw data. There are several other sensor network QoS definitions existing in the literature. As surveyed in [6] and [7], these WSN QoS definitions include both network QoS attributes such as latency, jitter, throughput and packet loss, and application level QoS attributes such as spatial resolution, coverage, exposure and system lifetime. The QoS perspective that we will use throughout this study covers four of the sensor network service quality attributes mentioned above, namely, spatial resolution, coverage, packet collision and network lifetime. In fact, we will build a QoS control strategy which mainly concentrates on the spatial resolution attribute as defined in [5]. Yet, at the end, we will show that the proposed strategy also takes care of other three QoS attributes.

For envisioned sensor network applications of near future, another requirement, which is also as important as QoS, is an effective security mechanism. Since sensor networks may be in interaction with sensitive data or operate in hostile unattended environments like battlefields, protection of sensor data from adversaries is an inevitable requirement. Similarly, for commercial applications of WSN, the protection of privacy such as personal physiological and psychological information is equally important. Because of inherent resource and computing limitations of sensor networks, however, traditional security techniques cannot be

used directly. There are several studies such as [8], [9] and [10]which propose security solutions tailored for sensor networks.

In the previous two paragraphs, we mentioned research studies which consider QoS for sensor networks ([5], [6], [7]) and security for sensor networks ([8], [9], [10]). Only a few articles on WSN such as [11], [12] and [13] deal with QoS and security at the same time but all from a constrained viewpoint which only analyze the effect of applied security mechanisms on the performance of the sensor networks. In fact, to the best of our knowledge, other than our previous paper [1], there is only a single work [14] which tries to simultaneously control security and QoS levels of a sensor network. Yet, defining QoS as network performance, the study presented in [14] has a different scope from our approach since here we consider only application level QoS attributes.

Our overall aim in this study is to present a novel control strategy that will outperform the method in [1], which was mainly based on ACK strategy of [15]. This new strategy will satisfy the time-varying QoS and security requirements of a wireless sensor network during its entire operation. In other words, the proposed strategy of this work aims to keep a sensor network at required spatial resolution and security levels, and at the same time, provide sufficient coverage by distributing active (data-sending) sensors uniformly over the field. The proposed approach also aims to maximize the network lifetime by implementing a power-aware algorithm and to minimize packet collisions by utilizing a slotted MAC scheme. In addition, the strategy presented also includes the solution of an optimization problem by a heuristic to determine optimal tradeoffs between security and spatial resolution.

The remainder of this paper is organized as follows: Section 2 surveys the related work that we utilized to develop our new QoS and security control strategy. Section 3 presents the scope of this study describing the assumptions, system model and problem formulation.. In Section 4, we give the details of the relationship between security and spatial resolution and also the heuristic for determination of best security-spatial resolution combinations. Section 5 is where we present the proposed strategy followed by the simulation results in Section 6. We finally conclude in Section 7 by summarizing intended future extensions to this study.

2 RELATED WORK

[5] is one of the initial analysis which introduce quality of service concept for wireless sensor networks. It defines sensor network QoS in terms of how many of the deployed sensors are active in sending data to the information sink. In this way, QoS concept is taken to be the same as spatial resolution, which is the amount of useful information that can be constructed by the aggregation of data sent by individual sensor nodes.

The main purpose of the research in [5] is to control the sensor network in such a way that the optimal spatial resolution level, which is known a priori, is attained during the sensor network operation period. Besides, in order to maximize the network lifetime, active sensors contributing to the spatial resolution are periodically changed to distribute power usage among all available sensors. To accomplish this goal, authors utilize a statistical paradigm called *Gur Game*. In the proposed control strategy of [5], a central authority, i.e. cluster head of a cluster-based sensor network, periodically broadcasts a probability at discrete time intervals. Each sensor compares this probability value to its locally generated random number for the current time interval and based on this comparison, jump between the states of a finite state automaton called Gur Memory.

In [15], authors present an alternative to the Gur Game strategy of [5] to be used in controlling the QoS level of a sensor network. The network topology assumptions and QoS definition are exactly the same in both studies, i.e., a cluster-based sensor network is considered and QoS is taken to be equal to spatial resolution. The main difference of [15] is its control scheme which is not dependent on broadcasts by the cluster head. Named as ACK strategy, proposed control method of [15] relies on cluster head's unicast messages to only transmitting nodes allowing non-transmitting nodes to shut down their radios, thus providing energy efficiency.

In ACK strategy, each sensor is associated with a finite state automaton as illustrated in Figure 1. Each state i of the automaton corresponds to a different transmit probability Ti such that $Ti > Tj$ for $i>j$. At each discrete time interval (epoch), each node compares its locally generated random number to the transmit probability corresponding to its current state i.

Then, each node decides whether to transmit or not in the current epoch based on this comparison. At the end of each epoch, cluster head counts the number of packets it received during this epoch and compares this value to the desired spatial resolution value. Cluster head sends the result of this comparison in an ACK packet to only active nodes which transmitted in the epoch. On receiving this acknowledgement packet, transmitting nodes change their states based on the 1-bit information in the ACK packet. They reward themselves if the bit is 1 meaning that number of transmitting nodes is lower than desired spatial resolution and they punish themselves otherwise.

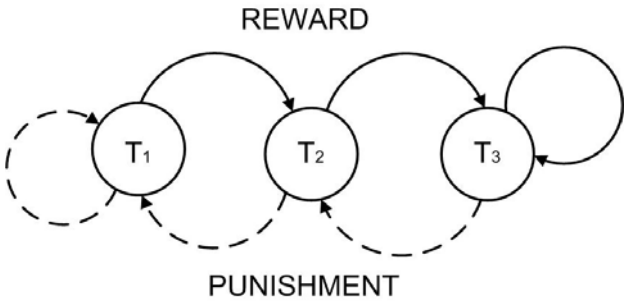

Fig. 1. Finite state automaton for ACK strategy of [15].

As a result, ACK strategy of [15] causes transmitting nodes to adjust their transmit probability according to the difference between current and desired levels of spatial resolution. So, in the steady state the sensor network is expected to converge to desired spatial resolution value. Since non-transmitting nodes can turn off their receivers at the beginning of each epoch, ACK strategy enhances power conservation. Still, however, all nodes are ON at any moment in the sense that they all generate random numbers and compare these to their transmit probability. Authors have shown that ACK strategy of [15] outperforms the Gur Game method of [5] more than five times regarding total network life.

In [1], a security and QoS control strategy based on the ACK method of [15] is presented. Inheriting the spatial resolution providing and power conserving features totally from the ACK method, the proposed strategy of [1] has also provided security by appending TinySec [11] message authentication codes to transmitted packets and minimized packet collisions through the use of a slotted MAC scheme. In the simulation results, it was shown that the proposed control method of [1] provided also some statistical assurance on coverage.

[1] is one of the initial works providing security and application level QoS simultaneously. However, there are some problematic issues in the control algorithm of [1]. One of those problems is the following: Though it is able to have all packets transmitted at the required security level, the control method of [1] cannot make the network attain exactly the desired spatial resolution levels, i.e., at some times, the achieved resolution value is below the required one. This is due to the non-zero spatial resolution variance values of the Markovian modeling of the ACK-based network detailed in [15]. Another issue in the control method of [1] is the unequal participation of available sensor nodes in the data transmission process. In other words, for some periods, some sensors transmit packets more frequently while others hardly ever transmit. This results in unbalanced battery dissipation among the nodes and causes some nodes to die sooner. Although previously less active nodes start transmitting instead of the dead nodes after a while, it takes some time for the network to reach back to the desired resolution value. What is worse, there is a tradeoff between variance and equal participation of nodes, diversity as called in [15], and this fact makes it very difficult to provide required spatial resolution and balanced power usage for lifetime maximization at the same time for the control method presented in [1].

The mentioned drawbacks of [1] are all due to the utilization of ACK-based strategy of [15]. So, in this paper we propose a novel QoS and security control strategy not based on the ACK method. We design our new method to be free from limitations of [1], that is, to provide desired resolution at all times and to have even power consumption among sensors for system lifetime extension. In addition, we also expect to enhance coverage performance by making a more even geographical distribution of transmitting sensors over the field.

3 SCOPE OF OUR WORK

In this section, we are going to define the scope of our work. First, we will give our assumptions about the underlying network infrastructure and our security and service quality perceptions. Then, we will attempt to present a clear and exact description of the problem to which our proposed strategy offers a solution.

3.1 Assumptions and System Model

Before giving our problem description, we will specify our assumptions regarding the topology of sensor network that we consider, communication model of this network and properties of security and spatial resolution concepts as we use in this paper.

3.1.1 Topology Assumptions

We assume a clustered sensor network topology similar to the one used in the LEACH architecture [16]. In this topology, overall network is divided into non-overlapping clusters. In each cluster, there is a cluster head located in the communication range of all sensors in this cluster. All sensors can send their data directly (in one hop) to their corresponding cluster head. Each cluster head aggregates the data received from sensors and send this aggregated data to the sink possibly over other cluster heads in a multi-hop fashion.

In this paper, we consider only one single cluster of such a network and try to control the security and spatial resolution levels for just this single cluster. Questions such as how clustering is performed, how cluster heads communicate with each other and with the sink, and how data aggregation is performed are all beyond the scope of this study.

3.1.2 Communication Model

In order to take advantage of the existence of a central entity (cluster head) to reduce packet collisions, we prefer to use a centralized MAC scheme rather than purely contention-based distributed schemes such as ALOHA or CSMA. Since fixed-assignment based MAC strategies like pure TDMA may cause channel inefficiency due to empty slots assigned to non-transmitting sensors, our assumed MAC scheme is a demand-based one. Among demand-based MAC methods, we prefer a reservation-based one in which time is divided into frames each of which is composed of two main parts named as reservation period and data transmission period. Reservation period is where stations wanting to transmit contend for an empty mini slot. Then, in data transmission period which is composed of multiple data slots, stations that have accessed an empty mini slot during the reservation period send their data in their assigned data slot. There are several reservation-based MAC schemes proposed for

sensor networks such as DR-TDMA [17] and TRACE [18]. In this paper, we use a version of TRACE that we have modified to suit our specific needs. We leave detailed explanation of our MAC scheme to next section and proceed with our assumptions on the communication model.

We assume that total channel capacity of the cluster under question is limited and this limit is known in advance as bits per second. Sensors are allowed to send their data in their assigned slot of the MAC frame. Each sensor is assigned one and only one data slot in each frame and in each data slot, a sensor transmits only one single packet. We assume TinyOS type packets composed of a data part and an overhead part. Data part has constant length. Overhead part has variable length due to the security overhead which increases as security level increases. This varying length security overhead causes the overall packet to be of varying length. Therefore, the length of the data slot assigned for a sensor's packet should also have non-constant length to accommodate packets of different security levels. However, total frame time and total data transmission period in each frame has constant duration in accordance with the upper bound of the channel capacity. This means that number of data slots that can be accommodated in a single frame is upper bounded. This upper bound is equal to the duration of data transmission period in a frame divided by duration of a single data slot. Therefore, number of active sensors sending data to the cluster head in one frame duration has also the same upper bound. Because the duration of a data slot varies with security level, this limit in number of active sensors is correlated with security level. The correlation between spatial resolution and security resulting from the capacity limits of underlying communication channel is an important point taken into consideration in our control strategy.

3.1.3 QoS Assumptions

We have previously stated that one of the main attributes of our QoS perception is spatial resolution, which is defined in [5] as the number of sensors that are active in sending data to the cluster head during a specified time. Though it is true that spatial resolution taken as number of active sensors is a measure of service quality, it does not by itself represent the overall sensor network QoS as assumed in [5] and [15] since geographic locations of individual sensors really matter. In fact, a high level of spatial resolution does not guarantee a

full coverage of the network, especially if active sensors are gathered in a particular region of the cluster under consideration.

Therefore, in this study, we consider spatial resolution and coverage together and also include two more service quality attributes such as packet collision rate and network lifetime. Actually, our focus is on spatial resolution in the sense that we propose a control strategy to maintain spatial resolution and security levels in a cluster-based sensor network. However, we design our control strategy such that it also takes care of other three QoS attributes given above.

Regarding spatial resolution, we assume that there are several spatial resolution levels to meet different requirements. In fact, spatial resolution N of the sensor network cluster can take any positive integer values between $Nmin$ and $Nmax$ which represent minimum and maximum defined spatial resolution levels respectively. $Nmin$ is the number of active sensors just enough to derive the minimum amount of information required for system functionality and $Nmax$ is the number of active sensors needed to derive the best quality information and further increase in N does not improve the information any further. $Nmin$ and $Nmax$ are system parameters determined by specific requirements of the sensor network.

3.1.4 Security Assumptions

In our study, we consider only the security of sensor to cluster head communication and assume communications from cluster head to sensors or to the sink are secured by other means. Our security definition includes only integrity and authentication of data packets sent by sensor nodes and does not include confidentiality.

Another assumption on security is that there are multiple security levels defined for our sensor network. Each security level is associated with a different length message integrity code (MIC). We represent security level with S and $S=0$ corresponds to lowest security level where no MIC is used and $S=Smax$ corresponds to highest security level where longest MIC is used. S can take any positive integer values between 0 and $Smax$.

Our final security assumption is that all sensors communicate at the same security level during a frame duration. It must also be noted that we should either be given or be able to compute length of the security overhead per packet for all security levels.

3.2 Problem Description

In this study, we consider a wireless sensor network which has simultaneous security and service quality requirements. Under the assumptions and constraints given in section 3.1, the problem to which a solution is presented in the next section is the following: To control the sensor network in such a way that time-varying security and QoS requirements are fulfilled during the entire operation. In other words, we have five main objectives: (1) to keep enough number of sensor nodes active (ON) to attain desired spatial resolution level, (2) to have these active sensors communicate at the required security level, (3) to maximize network lifetime by having active sensors periodically power down and inactive ones power up for a balanced energy dissipation, (4) to provide full coverage by having at least one sensor taking measurements on each geographical region and, (5) to minimize packet loss resulting from collisions.

The problem which comprises of only part (1) and (3) above, i.e. controlling spatial resolution and maximizing network life time has already been solved in [5] and [15]. In [1], security described in (2) above is appended as an additional parameter to this solution and also it is allowed that both desired spatial resolution and security requirements can change in time as needed. Moreover, the QoS concepts used in [5] and [15] are extended to include coverage as described in (4) and collision rate defined as (5). So, the QoS and security control strategy presented in [1], which is inspired from the ACK-based automaton of [15], provided a solution to achieve all five objectives above

Our contribution in this paper is to propose a novel control strategy to achieve all five security and service quality objectives without having the drawbacks of the method proposed in [1]. To elaborate, we seek to design a new QoS and security control strategy for wireless sensor networks which will provide closer values to required spatial resolution levels, longer network lifetime, and better coverage. So, our proposed method will enhance three of the QoS attributes, namely, spatial resolution, network lifetime and coverage, compared to the values

achieved in [1]. Moreover, it will utilize a much more computationally efficient heuristic algorithm to solve the optimization problem introduced in [1]. Before presenting the details of our proposed strategy, we give some information about the correlation between security and spatial resolution that will be used in the control algorithm of this paper.

4 RELATION BETWEEN SECURITY AND SPATIAL RESOLUTION

The solution of the problem described in Section 3 involves several challenges. The main challenge is to find a control strategy to keep the spatial resolution and security levels of the sensor network at the required values. However, as we have mentioned, there is a correlation between security and spatial resolution due to the fact that they both use up the same scarce resource, which is the channel capacity. Therefore, there might be cases where requested security and spatial resolution levels exceed the available channel capacity hence, cannot be supported by the network. So, another challenge to overcome is to find a way to check whether the required security and the required number of transmitting sensors can be supported. If they are not, then we need to determine the supported values which are closest to required values and then choose the optimal values among the supported ones. Therefore, as for the third challenge, we need a method to compute the optimal supported (security, spatial resolution) tuple which yield best tradeoff for cases when required security and spatial resolution levels exceed channel capacity.

The proposed spatial resolution and security control strategy of this paper, which we present in next section, is formed by the union of sub-solutions devised to overcome challenges given above. In the proceeding subsections, we first give these sub-solutions and then present our overall solution in next section.

4.1 Formulation of the Correlation between Security and Spatial Resolution

As mentioned in the previous sections, security adds some overhead bits due to the message integrity code appended to the end of the packet transmitted by sensor nodes. We have also indicated that this increase in packet size causes an increase in the data slot duration needed to transmit this packet. Since the duration of total data transmission period is fixed, increase in the durations of individual data slots result in a decrease in number of data slots

that can be accommodated in the data transmission period of a single MAC frame. Because each sensor can transmit during only one data slot of each frame, number of non-empty data slots in a frame is equal to the number of sensors that transmit in that frame, which is our spatial resolution definition. So, this fact proves that an increase in the employed security level during a specified time duration results in a decrease in spatial resolution for that time duration.

Yet, we still have to formulate this inverse relationship between security and spatial resolution to be able to determine what values of security and spatial resolution can be supported by the limited channel capacity of our sensor network. For this, we first need to specify the effect of security on packet length and data slot duration by determining data slot durations corresponding to each security level. Then, we should compute how many of these data slots can be accommodated in our MAC frame for each security level. These are given in the sequel.

4.1.1 Effect of Security on Packet Length

In Section 3.1.2, we have stated that we assume TinyOS packet format, details of which can be found in [11]. This type of packet has a total length of 36 bytes with 29 bytes of data, 5 bytes of communication overhead and 2 bytes of CRC. In the previous assumptions, we have defined our security concept as preserving integrity and authenticity of packets using message integrity codes (MIC). A security method suitable for our assumption is the authentication only (TinySec-Auth) option of TinySec sensor network security protocol proposed in [11]. According to the format of the TinySec-Auth packet, total length of a packet with 4-byte MIC appended is 37 bytes. So, security adds up only a 1 byte overhead to the data packet when TinySec-Auth is used.

TinySec protocol assumes only a single option for the length of MIC used as 4 bytes and this is not in accordance with our multi-level security assumption. Yet, there is no reason for not to extend the TinySec-Auth to allow multiple MIC length selections. In fact, the *security suite* feature of IEEE 802.15.4 specification [19] is an example of this multi-mode security approach. Among eight security suite options of IEEE 802.15.4, there are three authentication-only options with MIC sizes of 4, 8 and 16 bytes. So, we adopt this approach

and assume that we have four security levels one of which is no security and others include 4, 8 and 16 byte MICs. Knowing that a TinyOS packet with no MIC is 36 bytes and a TinySec-Auth packet with 4-byte MIC is 37 bytes, the relationship between security level *S* and corresponding packet length *Ps* is as given in Table 1.

Table 1. Packet lengths corresponding to different security levels

Security level *S*	Description	Packet length *Ps*
0	No security	36 bytes
1	4 bytes MIC	37 bytes
2	8 bytes MIC	41 bytes
3	16 bytes MIC	49 bytes

Before proceeding, we should note an important point about the generality of our work. Our proposed QoS and security control strategy is neither coupled to any of the above mentioned security methods nor limited to only 4 security levels. As long as the packet lengths *Ps* corresponding to each security level *S* is known, our strategy is applicable.

4.1.2 Relationship between Security and Spatial Resolution

After determining the packet lengths corresponding to each security level, we should now find the slot durations required for these packet lengths and how many data slots can fit into one frame for each security level. Both of these require a clear specification of the employed medium access control scheme.

We use a modified version of the reservation-based dynamic TDMA protocol named TRACE [18]. The symbolic representation for the frame format of our MAC scheme is given in Figure 2 for two frames. The only visible difference of our MAC frame from TRACE is the variable length data slot durations. In fact, we have two other differences as far as the type of information sent in Header part and Contention mini slots are concerned. But, we leave the explanation of these differences to later sections and continue with the basic operation of our MAC scheme.

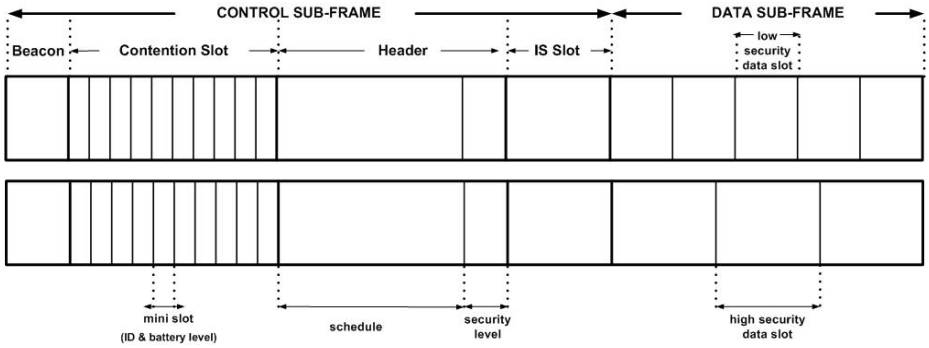

Fig. 2. The frame format of our MAC scheme (2 frames are shown)

Each frame consists of two sub-frames: a control sub-frame (reservation period) and a data sub-frame (data transmission period). The control sub-frame consists of a beacon message, a contention slot, a Header message, and an information summarization (IS) slot. Beacon message is used to synchronize all sensor nodes at the beginning of each frame. Contention slot consists of several mini slots and nodes that have data to send for this frame randomly choose one of these mini slots to transmit their request. Different from the original TRACE protocol where nodes transmit only their source ID during contention mini slots, in our MAC scheme, nodes give one more piece of information regarding their remaining battery level during contention period. If a node succeeds to win (i.e., no other sensor chooses the same mini slot) and if it finds its ID in the schedule announced in Header period, the contending sensor node can transmit its packet in the data transmission period without any collision risk. Following the contention period, the controller, i.e., cluster head, transmits the Header, which includes the data transmission schedule for the current frame. The nodes that will be included in the schedule are selected from the successfully contending nodes and nodes with higher battery levels are preferred. Unlike the original TRACE scheme, the Header includes additional information, which is the requirement for the current security level. The IS slot follows the Header slot and is used for partitioning of the network. Control sub-frame ends with the IS slot and data sub-frame begins.

The last difference of our MAC scheme from the original TRACE protocol is that data sub-frame is broken into variable length data slots for each transmission period or epoch. These data slots have variable lengths to accommodate different length packets of different security levels. In other words, the security level of all nodes during a frame duration is assumed to be the same, so all data slot lengths of the same frame are equal. However, the security levels of different frames may not be the same and therefore, the data slot lengths of

different frames may vary (see Figure 2). We represent the data slot length required to accommodate a packet at security level *S* with *Ds*. This *Ds* value is not the same as the packet length *Ps* because of the overheads required at each data slot. These overheads are usually due to preamble and synchronization bits and IFS (inter frame space). As in the original TRACE protocol, we assume a total of 6 bytes overhead for each data slot (4 bytes for packet header and 2 bytes for IFS guard band). So, our *Ds* values corresponding to the *Ps* values of Table 1 are *D0=42 bytes*, *D1=43 bytes*, *D2=47 bytes* and *D3=55 bytes*.

Now, what remains is to compute how many of these data slots can be accommodated in the fixed data sub-frame duration of a single frame. Representing the constant data sub-frame length with *DSF* and maximum number of data slots that can fit into a frame at security level *S* with *Ns,max*, the following inequality should hold not to exceed the channel capacity: $Ns,max \leq DSF/Ds$. Since we know the constant value *DSF* and have computed all *Ds* values, we are able to determine maximum spatial resolution that can be supported at security level *S,* which is *Ns,max*. And, the inequality $Ns,max \leq DSF/Ds$ is the relationship between security and spatial resolution that we were seeking. Representing security level requirement by *S** and spatial resolution requirement by *N**, we can easily check whether a required security-spatial resolution pair (*S*, N**) is supported by substituting these values into above inequality. If $N^* \leq DSF/Ds^*$, required levels are supported, otherwise they are not.

If we use our example network parameters together with a *DSF* value of 1050 bytes (coming from an assumption of 25 data slots can fit in a frame at no security, i.e., 25x42=1050), we can compute that *N1,max = 24, N2,max = 22, N3,max = 19* and we already know that *N0,max = 25*. Then, for example, (*S*, N**) = (*1, 23*), (*3, 15*) and (*2,20*) are supported whereas (*1, 25*), (*3, 20*) and (*2,23*) are not. Next subsection explains how we deal with such unsupported (*S*, N**) requirements.

4.2 Determination of Optimal Security and Spatial Resolution Values

We have just shown that there might be cases when required spatial resolution and security values cannot be attained. For such cases, we have to determine the supported values that are closest to the requirements. Yet, this is not a simple task since there usually exist more than one supported security-spatial resolution pair. Take the example case for a

requirement of (*S*, N**) = (*3, 25*) which cannot be supported. In this case, should we sacrifice security choosing supported pair of (*0, 25*), or sacrifice spatial resolution and choose (*3, 19*), or sacrifice from both sides and choose (*2, 22*).

In fact, determination of the best tradeoff for unsupported (*S*, N**) requirements is a resource allocation problem where the scarce resource is channel capacity and competing factors are security and spatial resolution. Such resource allocation problems are optimization problems which are studied in several works in the literature. One of such studies is [20] whose problem modeling fits into our setting. So, we will utilize their main approach which is based on finding the values which maximize an aggregate utility function. The aggregate utility function is a weighted sum of individual utility functions which reflect the marginal benefits of each factor competing for the scarce resource.

For our case, we have two individual utility functions for security and spatial resolution represented as *Us(S)* and *UN(N)*, respectively. These functions map the security and spatial resolution values in their defined range to a positive utility value representing the benefit provided by the corresponding security or spatial resolution value. The properties of such utility functions and information on how they can be constructed can be found in [20]. We assume that we are already given these utility functions *Us(S)* and *UN(N)*. Then, our overall utility function to be maximized is the weighted sum of those and equal to $U = Ws.Us(S) + WN.UN(N)$.

As a result, in order to determine optimal supported security and spatial resolution values when requirements cannot be satisfied, we should solve the optimization problem given in Equation 1 for *S* and *N*.

$$\begin{aligned} &\text{Maximize} \quad U = Ws.Us(S) + WN.UN(N) \\ &\text{Subject to} \quad N \le DSF/Ds, \\ &\qquad\qquad N^{*}min \le N \le N^{*}, \\ &\qquad\qquad S^{*}min \le S \le S^{*} \end{aligned} \qquad \textbf{(1)}$$

Here, *N*min* and *S*min* stands for the minimum required levels for spatial resolution and security. These are different than actual requirements represented by *N** and *S** and used for preventing the sensor network from operating at undesirably low security and spatial resolution levels. If the minimum requirements *N*min* and *S*min* cannot be supported, the sensor network ceases its operation until minimum requirements can be satisfied.

Since we have only two unknowns (*N* and *S*) and the possible values for these unknowns are both upper and lower bounded, for most cases, we can solve the above optimization problem by enumeration of the whole solution space. So, given an unsupported *(S*,N*)* pair, we can find the optimal supported pair *(S',N')* by trying all possible *(S,N)* combinations in the range $N^*min \leq N \leq N^*$ and $S^*min \leq S \leq S^*$ and pick the one yielding the maximal *U* value which also satisfies the condition $N \leq DSF/Ds$. More information on this brute force approach to solve the optimization problem of Equation 1 and effect of utility function parameters on the solution can be found in [21].

Yet, for cases where this brute force approach is not feasible, we propose a heuristic with a much more endurable computational complexity. The basis of our heuristic is the fact that the overall utility function *U* is a non-decreasing function of both *S* and *N* since individual utility functions *Us* and *UN* hold this property. This fact makes it unnecessary to check all *(S,N)* combinations in the range *[S*min, S*]* and *[N*min, N*]*. In fact, if one can find a tuple *(N',S')* satisfying all three constraints defined by three inequalities of Equation 1, then it is unnecessary to check also *(N'-k, S'-m)* for any $k \geq 1$ and $m \geq 1$ because the utility value *U(N',S')* is always greater than or equal to utility value *U(N'-k, S'-m)* due to non-decreasing feature of utility functions mentioned before. The heuristic algorithm developed on this basis is given below.

Heuristic(*N*,S**)

1.*Uold := 0*

2.*Unew:=0*

3.*S=S*;*

4.**while (***N* >= Nsmax(S-S*min)* **and** *S>S*min)* **do**

5. *N := Nsmax(S-S*min)*

6. *Unew := Ws.Us(S-S*min) + WN.UN(N-N*min)*

```
7.  if (Unew>Uold) then
8.      Uold := Unew
9.      Noptimum := N
10.         Soptimum := S
11.     S :=S-1
12.  if (N* >Nsmax(S-S*min)) then
13.     N := Nsmax(S-S*min)
14.  else
15.     N=N*
16.  Unew := Ws.Us(S-S*min) + WN.UN(N-N*min)
17.     if (Unew>Uold) then
18.         Noptimum := N
19.         Soptimum := S
20.  return Noptimum, Soptimum
```

5 PROPOSED QOS AND SECURITY CONTROL STRATEGY

As stated previously, the control strategy of this paper aims to provide five attributes for cluster-based wireless sensor networks, which are security, spatial resolution, maximal network lifetime, minimal packet loss and sufficient coverage. To provide best performance for the achievement of those attributes, we tried to utilize the existence of a central entity, cluster head, in the most efficient way. However, instead of making the cluster head apply a direct control on sensors, we let each sensor make its decision on packet transmission individually and then the cluster head makes the final selection. Under the guidance of incentive stated above, we applied the following principles while designing our control strategy:

- If our method can cause enough (more than *N*)* number of sensors to show their intent to transmit at each MAC frame, then cluster head can choose a certain number (exactly *N**) of sensors to transmit. This will provide desired *spatial resolution* value at each frame duration. In our method, each sensor node *i* independently decides to transmit or not for each frame duration by comparing its locally generated random number to a probability value *Pi*. To

make more than N^* sensors intend to transmit, each node will update its probability value at each frame using the following rules.

- If a node has decided to transmit and its name is included in the data transmission schedule, the probability value *Pi* for this node will not be changed. (Since this case will usually occur when number of nodes wanting to transmit is just fine to provide required spatial resolution level, there is no need to change transmit probabilities.)
- If a node has decided to transmit but its name is not included in the data transmission schedule, the probability value *Pi* for this node will be decreased. (Since this case will usually occur when number of nodes wanting to transmit is above the required spatial resolution level, transmit probabilities must be decreased.)
- If a node has not decided to transmit, the probability value *Pi* for this node will be increased. (This is to prevent nodes from remaining passive for long periods of time and intends to provide equal power consumption of available sensors.)

- In order to further contribute to balanced energy dissipation, our method will use the battery level information of sensor nodes which they state during contention period. This battery level information is just two bits for each node, which makes up four battery levels such as very low, low, high and very high. So, among the nodes accessing contention mini slots, N^* of them having highest battery level will be selected to transmit. This way, battery consumption of nodes will be evenly distributed in time providing *longer lifetime*.
- In the Header period of MAC frame, desired security level of current period is announced to nodes that will transmit data for that frame. All sensors should send their data with a message integrity code corresponding to announced security level. This will provide *security* of sensor to cluster head communications.
- Since the slotted MAC algorithm that we use allows transmission of only the selected nodes in their corresponding data slots, there is no risk of collision during the data sub-frame. Also, the number of contention slots will be designated to be sufficiently higher than the number of data slots and this will further reduce the collisions that can occur during control sub-frame. So, proposed control method will *minimize packet collision* rate.
- For coverage, our method will not involve any direct control mechanism. Yet, we expect that the stochastic nature of our strategy causing each sensor *i* to make transmissions based on an independent probability value *Pi* will result in a geographically balanced distribution of active nodes. So, our proposed method is also expected to provide sufficient *coverage*.

Before proceeding with the operational steps of our proposed quality of service and security control strategy, here are some final words about the setting. The initial values for the probability value *Pi* for each node *i* is set to *Nmax/Ninitial* where *Nmax* is the maximum defined spatial resolution value and *Ninitial* is the total number of sensors initially deployed. The increment *inc* that will be used to update *Pi* can be set to any value greater than zero and smaller than 0.5. Time is divided into discrete intervals named as epochs. Duration of each epoch is equal to one frame duration of our MAC scheme and epochs are synchronized with frames. During each epoch, the following events occur in the given order.

1. Cluster head (CH) starts transmitting the beacon message.
2. CH checks whether there is a change in the required security and spatial resolution levels *(S*,N*)* which are announced by the control center of the sensor network. If there is a change in either *S** or *N** with respect to previous epoch, CH proceeds to step 3, otherwise it goes to step 6.
3. CH checks whether new security and spatial resolution requirements are supported by using the method given in section 4.1.2. If they are supported it goes to step 6. If required levels *(S*,N*)* are not supported, it computes the optimal supported levels *(S', N')* by the method of section 4.2 and then proceeds to step 6.
4. Before the beacon period ends, each and every nodes decides whether to transmit or not during the current epoch. Nodes make this decision by comparing their locally generated random number to the current value of probability *Pi*. Nodes which decide to transmit open their radio, synchronize with the beacon and proceed to step 5. Others shutdown their radio.
5. After the beacon period ends, nodes deciding to transmit in the previous step contend for a mini slot in the contention slot by sending their ID number and 2-bits battery level information during a mini slot.
6. Before the transmission of Header packet, CH should have finished the calculation of optimal security and spatial resolution values *(S', N')*. Also, in this step, CH determines the source ID's and battery levels of sensors that want to be active for the current epoch by checking the accessed mini slots of the contention period. Number of nodes desiring to transmit will be represented as *Nt* for epoch *t*.
7. During the Header period, CH unicasts the schedule of data transmissions for the current frame. This schedule is an ordered list of sensor nodes with corresponding node ID's and it also includes the slot duration *Ds* corresponding to desired security level of current epoch. CH

determines the sensor nodes to be included in the data transmission schedule in the following way. If *Nt* is smaller than both *N** and *Ns,max*, maximum supported number of active sensors, CH includes all of the *Nt* nodes in data transmission schedule. If *Nt* exceeds *N** but is smaller than *Ns,max*, then CH chooses only *N** of the sensor nodes among *Nt* nodes by giving priority to the ones with higher battery level. If *Nt* exceeds both *N** and *Ns,max*, then CH selects *Ns,max* sensor nodes with highest battery level to include in the announced schedule. If battery levels of two or more nodes are same, CH makes a random selection among them.

8. After the schedule is announced, CH informs nodes that want to transmit about one more issue during the Header period, which is the desired security level of current epoch (*S** or *S'*). Information on the security level occupies 2 bits since we assume 4 security levels. Yet, it may be increased if more security levels exist (i.e., 3 bits for 8 levels).
9. Each alive sensor node *i* updates its probability value *Pi* in the following way. If it has not desired to transmit for this epoch, then it sets *Pi= max(Pi+inc,1)*. If it has desired to transmit but its name was not announced in the data transmission schedule, then it sets *Pi= min(Pi-2*inc,0)*. Otherwise, sensor does not modify *Pi*.
10. All the sensor nodes which are not listed in the announced transmission schedule shut down their radio. Only the nodes which find their name in the schedule transmit their packets at the security level announced and in the data slot assigned to them.
11. After the data sub-frame ends, all sensor nodes return to step 4 and CH returns to step 1.

6 SIMULATIONS AND ANALYSIS

In order to see the performance of our proposed service quality and security control method whose operational steps are given in previous section, we performed some simulations using our own code written in MATLAB. For those simulations, we use the assumptions and system model given in previous sections, i.e., a single WSN cluster where sensors send data to the designated cluster head in one hop under TRACE based MAC scheme. In all cases, we have an initial deployment with *Ninitial*=100 sensors and use following network parameters: *Smin=0, Smax=3, Nmin=15, Nmax=35, Pi(t=0)=0.35, inc=0.05, N0,max = 25, N1,max = 24, N2,max = 22, N3,max =19, Ws=*W_N*=1, Us(S)= 1-(exp(-2.07*S-0.69))* and $U_N(N)=0.025*N+0.125$. More information on how we set utility function parameters is given in [21].

The results of simulations are shown below in Figures 3 to 6. In all the plots, we show the result produced under ACK-based method of [1] in upper part of the figure whereas results belonging to proposed method of this paper is given in the lower part.

Figure 3 illustrates the performance of the proposed strategy in controlling spatial resolution and Figure 4 in controlling security, under time-varying security and spatial resolution requirements. In Figure 3 and Figure 4, dashed lines represent required levels (*S* & N*),* dotted lines marked with squares represent supported levels (*S' & N')* computed using the heuristic given in Section 4 and continuous lines represent attained levels (*S & N).*

As can be seen from the lower part Figure 3, our proposed control method is able to exactly attain the supported spatial resolution level from beginning until the death of the network when number of alive sensors is less than minimum supported resolution level *Nmin*. However, there are several spike-like parts in the attained resolution graph of ACK-based method. This is mostly due to previously mentioned non-zero variance and unequal participation of nodes properties of ACK strategy [15]. Since our strategy does not utilize ACK method and relies on the simple idea of making a bit more number of sensors want to transmit than required resolution value and then select just required number of them, it is able to provide a spike-less, smooth appearance for attained spatial resolution graph. So, the proposed method is much better than method of [1] in providing spatial resolution. In fact, proposed method is able to provide the desired (required/supported) spatial resolution value for 8389 of the 8401 epochs where network is operational whereas the corresponding figure is 5769 out of 8226 for ACK-based approach. Another important point to note from those numbers is that the total lifetime of the network achieved with proposed method is longer than the one for method in [1], i.e., 8401 versus 8226 epochs. Before illustrating the main reason behind this lifetime extension, we will compare the security levels provided by both methods. As Figure 4 shows, performance of two methods regarding security is the same, that is, attained level *S* exactly traces the supported security value *S',* because both strategies force all active sensors to transmit at the required or supported security level.

Returning back to the network lifetime, Figure 5 gives information about the battery consumption of sensor nodes for proposed method and the method of [1]. Top graph of Figure 5 shows the battery level of sensors when network controlled by the method of [1] dies and

middle graph illustrates the same case for proposed method of this paper. As can be observed, battery dissipation of sensors under control of ACK-based strategy is very unbalanced since living nodes have lots of unused battery. This is due to previously mentioned low diversity problem of ACK strategy. Yet, for our method, at the end of the life of the network, almost all nodes have run out of battery indicating a balanced power dissipation among all sensors. This even distribution of battery levels indicating an equal contribution of sensor nodes to spatial resolution becomes more obvious in last graph given in bottom part of Figure 5 which illustrates battery levels of two nodes throughout their lifetime for both methods. Represented by solid lines, batteries of sensors under control of proposed method are consumed in a very balanced fashion. Starting with full batteries at startup, both sensors are able to distribute usage of their battery almost until the network dies, indicated by diagonal-like shape of the graphs. However, for ACK-based strategy of [1], some of the sensors do not use their batteries until a specific time, i.e., does not transmit at all, and thereafter they quickly consume up their battery, most probably due to continuous data transmission for some period. This is illustrated by two dotted lines in the graph. So, Figure 5 indicates that our proposed method performs well at providing balanced battery dissipation of all nodes and this results in a longer network life.

Finally, in Figure 6, we present the results regarding the coverage performance of our proposed strategy. In this case, we divide our sensor network cluster into four geographic sub-regions over which sensors are initially deployed in a random but uniform way. Then, we simulate this setup with the same parameters/requirements of previous case and observe the geographic distribution of active sensors contributing to spatial resolution over those four sub-regions. As illustrated in Figure 6, owing to the statistical nature of both ACK-based method of [1] and proposed method, active sensors are said to be evenly distributed and in each sub-region there are more than one active sensors most of the time. But, it can easily be seen from the graphs that distribution of active sensors in time and space is much more even for the case of our method. In fact, there are several cases when number of transmitting sensors drop to very low values (even to zero for sub-region 2) for ACK-based method whereas an equal average value is maintained almost all the times for the proposed method. This is an indication of better coverage for our method since there are more active sensors taking measurements in all of the geographic regions. Of course, however, the probabilistic approach

that we take to determine which sensors will be active does not provide a hard guarantee such that full coverage is ensured at all times.

So far in this section, we have shown the proposed strategy of this study performs well in maintaining security and spatial resolution levels (Fig.3 and 4), extending network lifetime (Fig.5) and finally providing coverage (Fig.6). Regarding the packet collision rate, we have not performed any simulations. Yet, in our MAC protocol based on TRACE [18], the probability of contention in the data slots is zero because data slots are dedicated to successfully contending nodes of the control sub-frame. Also, the number of contention slots is higher than the number of data slots and this further reduces the collisions that can occur during control sub-frame. So, our solution proposal also minimizes packet collision rate.

7 CONCLUSION AND FURTHER WORK

In this paper, we presented a novel control strategy for cluster-based sensor networks to maintain required security and service quality levels consisting of four attributes, which are spatial resolution, coverage, system lifetime and collision rate. Through simulations, we have shown that proposed method provides better performance compared to previous studies regarding three of the QoS attributes, namely, resolution, coverage and network life time. In addition, the method proposed in this paper is less complicated and simpler compared to more recent studies than [15] such as [22], [23], [24] and [25]. As opposed to those other studies, QoS control steps of this paper's strategy does not involve the solution of any linear programs or optimization problems and therefore, it is more likely to be implemented in real sensor platforms which have constrained computational and communication resources. In this work, we have also analyzed the correlation between security and spatial resolution and computed the best tradeoff for cases where network capacity is not sufficient to support required security and spatial resolution levels. We have done this computation by solving an optimization problem by the use of a heuristic algorithm also developed in this study. As further work, we plan to extend the proposed strategy to control security and service quality for multiple clusters of a sensor network.

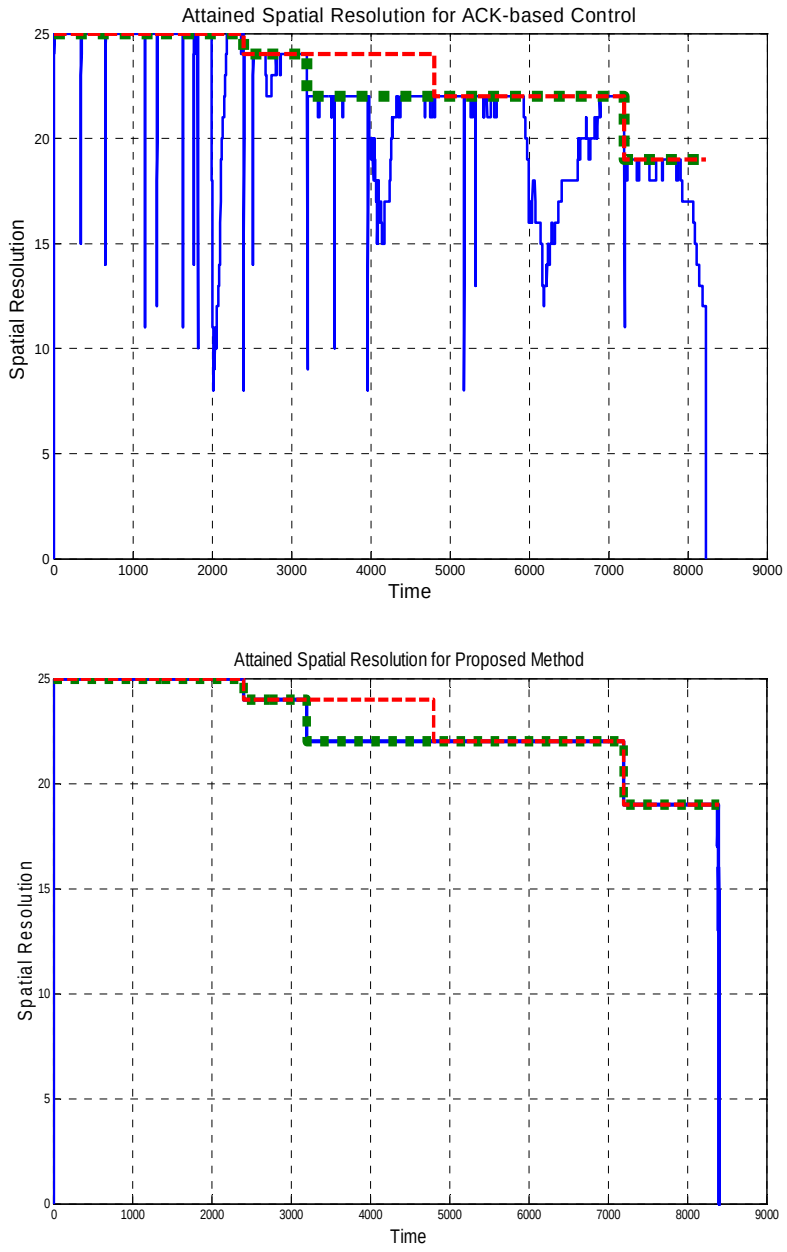

Fig. 3. Spatial resolution vs time for both methods

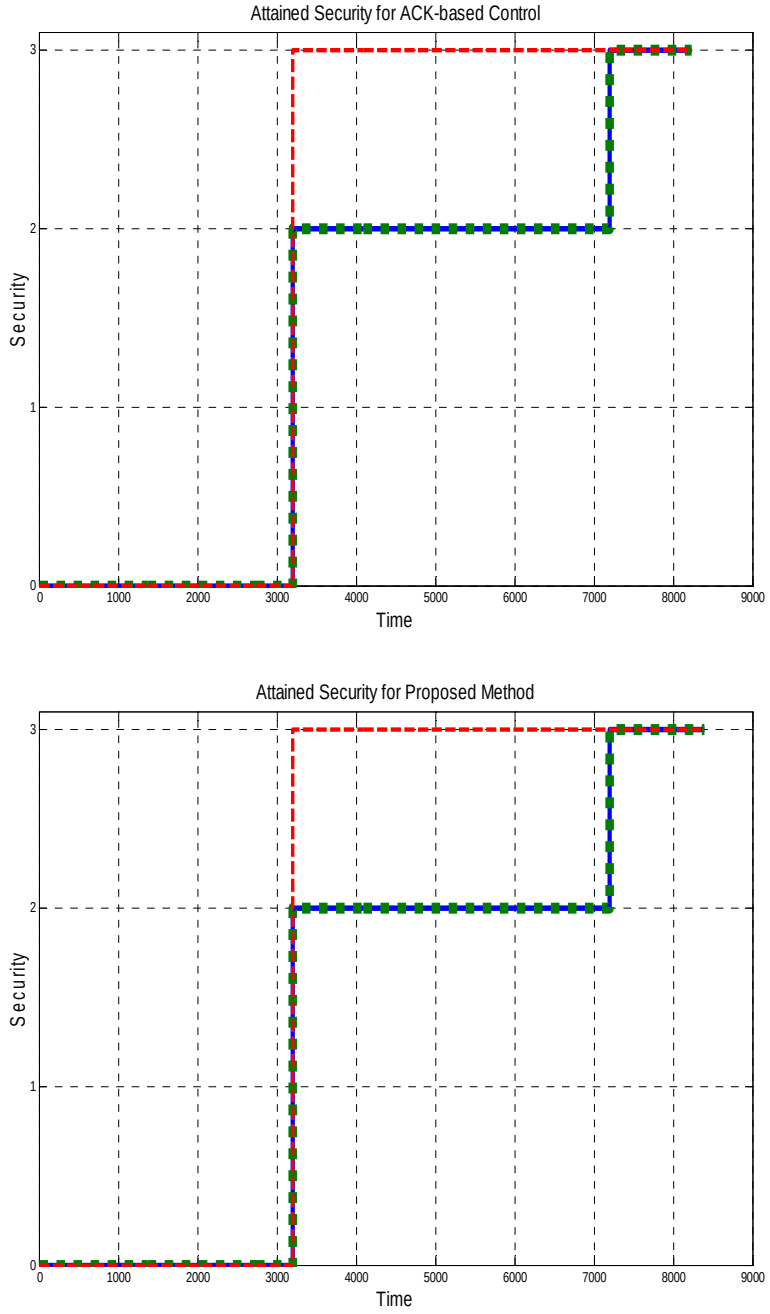

Fig. 4. Security vs time for both methods

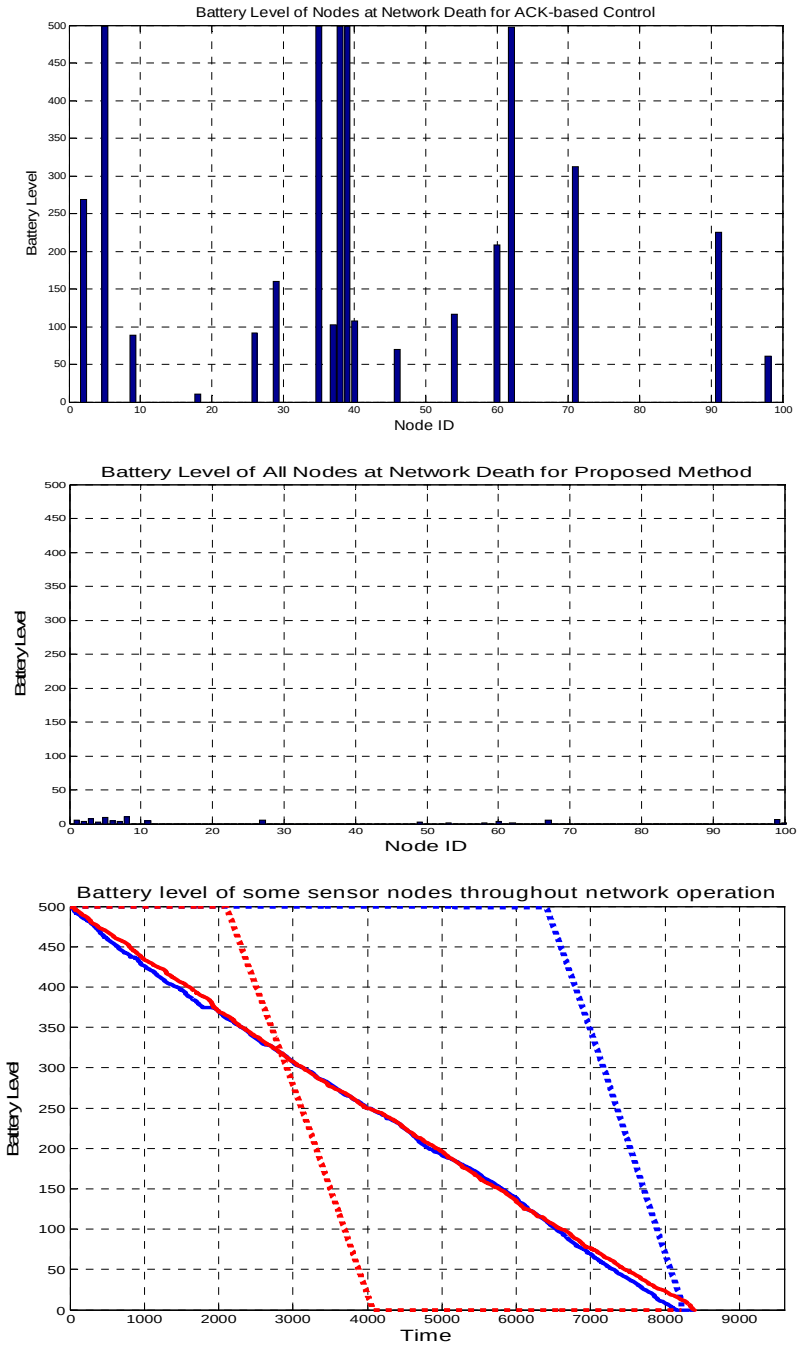

Fig. 5. Battery level of nodes for both methods

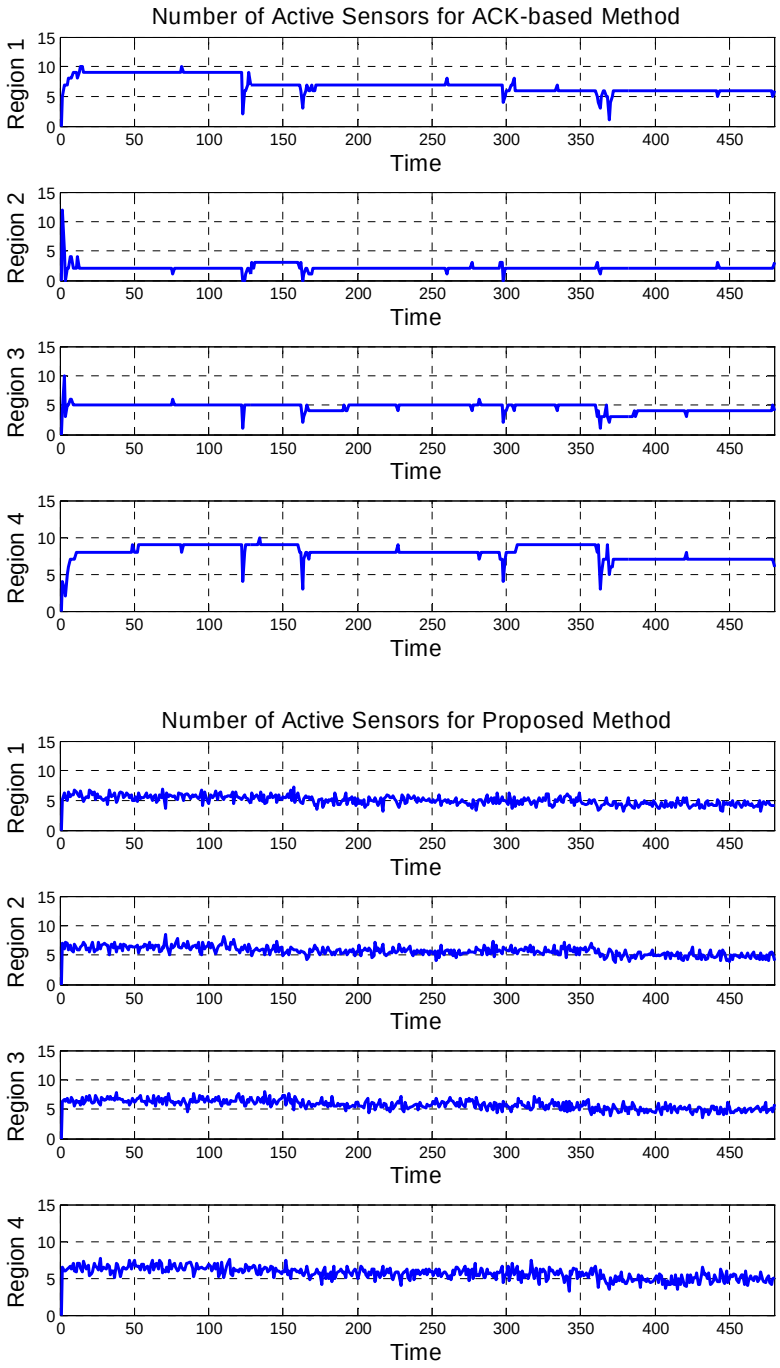

Fig.6. Distribution of active sensors over sub-regions

REFERENCES

1. Tomur, E., Erten, Y.M.: Security and Service Quality Analysis for Cluster-Based Wireless Sensor Networks. In: Proceedings of 5th International Conference on Wired and Wireless Internet Communications (WWIC 2007), (May 2007)
2. Shah, R., Rabaey, J.: Energy Aware Routing for Low Energy Ad Hoc Sensor Networks. In: Proceedings of IEEE Wireless Communications and Networking Conference, Orlando, FL (March 2002)
3. Younis, M., Youssef, M., Arisha, K.: Energy-Aware Routing in Cluster-Based Sensor Networks. In: Proceedings of the 10th IEEE/ACM Sym. on Modeling, Analysis and Simulation of Computer and Telecomunication Systems (MASCOTS'02), Fort Worth, TX (October 2002)
4. Jolly, G., Younis, M.: Energy Efficient Arbitration of Medium Access in Sensor Networks. In: Proceedings of the IASTED Conf. on Wireless and Optical Comm. (WOC 2003), Banff, Canada (July 2003)
5. Iyer, R. and Kleinrock, L.: QoS Control for Sensor Networks. In: Proceedings of IEEE International Communication Conference (ICC 2003), Anchorage, AK (May 2003)
6. Wang, Y., Liu, X., Yin, J.: Requirements of Quality of Service in Wireless Sensor Networks. In: Proceedings of the International Conference on Networking, Systems, Mobile Communications and Learning technologies (ICNICONSMCL06), (2006)
7. Chen, D., Varshney, P. K.: QoS Support in Wireless Sensor Networks: A Survey. In: Proceedings of International Conference on Wireless Networks (2004)
8. Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S. , Srivastava, M. B.: On Communication Security in Wireless Ad-Hoc Sensor Networks. In: Proceedings of International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WET ICE 2002), Pittsburgh, PA (2002)
9. Zhu, S., Setia, S., Jajodia, S.: Leap: efficient security mechanisms for large-scale distributed sensor networks. In: Proceedings of the 10th ACM conference on Computer and communications security, ACM Press (2003)
10. Carman, D. W., Kruus, P.S., Matt, B. J.: Constraints and Approaches for Distributed Sensor Network Security (Final). In: Technical Report 00-010, NAI Labs (2000)
11. Karlof, C., Sastry, N., Wagner, D.: TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. In: Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems (November 2004)

12. Guimarães, G., Souto, E., Kelner, J., Sadok, D.: Evaluation of Security Mechanisms in Wireless Sensor Networks. In: Proceedings of International Conference on Sensor Networks (August 2005)

13. Deng, J., Han, R., Mishra, S.: A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks. In: Proceedings of 2nd IEEE International Workshop on Information Processing in Sensor Networks (2003)

14. Chigan, C., Ye, Y., Li, L.: Balancing Security Against Performance in Wireless Ad Hoc and Sensor Networks. In: Proceedings of IEEE Vehicular Technology Conference (2005)

15. Kay, J., Frolik, J.: Quality of Service Analysis and Control for Wireless Sensor Networks. In: Proceedings of 1st International Conference on Mobile Ad-Hoc and Sensor Systems, Ft. Lauderdale, FL. (Oct. 25-27, 2004)

16. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: 33rd Annual Hawaii International Conference on System Sciences (2000)

17. Frigon, J.-F., Chan, H.C.B., Leung, V.C.M.: Dynamic reservation TDMA protocol for wireless ATM networks. In: IEEE JSAC, vol. 19, pp. 370-383 (Feb. 2001)

18. Tavli, B., Heinzelman, W.: TRACE: Time Reservation Using Adaptive Control For Energy Efficiency. In: IEEE Journal on Selected Areas in Communications, Vol. 21 (2003)

19. Wireless medium access control and physical layer specifications for low-rate wireless personal area networks. IEEE Standard, 802.15.4-2003, May 2003. ISBN 0-7381-3677-5.

20. Lee, C., Lehoczky, J., Rajkumar, R., Siewiorek, D.: On Quality of Service Optimization with Discrete QoS Options. In: Proceedings of the Fifth IEEE Real-Time Technology and Applications Symposium (1999)

21. Tomur, E., Erten, Y.M.: Tradeoff Analysis and Optimization of Security and Spatial Resolution for Sensor Networks. In: Proceedings of 41st Annual Conference on Information Sciences and Systems (CISS'07) (March 2007)

22. Delicato, F., Protti, F., Pirmez, L., de Rezende, J. F.: An efficient heuristic for selecting active nodes in wireless sensor networks. Computer Networks, 50(18), 3701 – 3720 (2006).

23. Zhou, J., Mu, C.: A Kind of Application-Specific QoS Control in Wireless Sensor Networks. In: Proceedings of IEEE International Conference on Information Acquisition (pp. 456-461) (2006)

24. Martínez J., Garcí A., Corredor I., López L., Hernández V., Dasilva A.: QoS in wireless sensor networks: survey and approach. In: Proceedings of the 2007 Euro American conference on Telematics and information systems (2007)
25. Akyildiz, I.F., Melodia, T., Chowdhury, K.R.: A survey on wireless multimedia sensor Networks Computer Networks. Vol. 51, No. 4., pp. 921-960 (2007)