# Architecture Design of Mobile Access Coordinated Wireless Sensor Networks

Mai Abdelhakim[1] Leonard E. Lightfoot[2] Jian Ren[1] Tongtong Li[1]
[1]Department of Electrical & Computer Engineering, Michigan State University, East Lansing, MI 48824, USA.
[2] Air Force Research Laboratory, Wright-Patterson Air Force Base, Dayton, OH, 45433 USA.

***Abstract*—This paper considers architecture design of mobile access coordinated wireless sensor networks (MC-WSN) for reliable and efficient information exchange. In sensor networks with mobile access points (SENMA), the mobile access points collect information directly from individual sensors as they traverse the network, such that no routing is needed in data transmission. While being energy efficient, a major limitation with SENMA is the large delay in data collection, making it undesirable for time-sensitive applications. In the proposed MC-WSN architecture, the sensor network is coordinated by powerful mobile access points (MA), such that the number of hops from each sensor to the MA is minimized and limited to a pre-specified number through active network deployment and network topology design. Unlike in SENMA, where the data collection delay depends on the physical speed of the MA, in MC-WSN, the delay depends on the number of hops and the electromagnetic wave speed, and is independent of the physical speed of the MA. This innovative architecture is energy efficient, resilient, fast reacting and can actively prolong the lifetime of sensor networks. Our simulations show that the proposed MC-WSN can achieve higher energy-efficiency and orders of magnitude lower delay over SENMA, especially for large-scale networks.**

***Index Terms*—Mobile access coordinator, wireless sensor networks, sensor network security and reliability.**

## I. INTRODUCTION

Wireless sensor networks have received significant attention from the research community due to their potential impact on various military and civilian applications. For efficient and reliable communication over large-scale networks, sensor networks with mobile access points (SENMA) was proposed in [1]. In SENMA, the mobile access points (MAs) traverse the network to collect the sensing information directly from the sensor nodes; when the energy consumption at the MAs is not of a concern, SENMA improves the energy-efficiency of the individual sensor nodes over ad-hoc networks by relieving sensors from the energy-consuming routing functions [1], [2].

While being energy efficient, a major limitation with SENMA is the large delay in the data collection process. This delay depends on the physical speed of the MA and the length of the MA trajectory, which would increase dramatically as the network size increases. Large delay makes SENMA undesirable for time-sensitive applications.

Along with the recent advances in the remote control technologies, UAVs have been used for management and coordination functions in wireless networks. For example, network deployment through UAV has been recently explored in the literature [3], [4]. For sensor deployment, the UAV basically carries one or more sensor nodes, then flies to the required location and gets down to a specific altitude where it is safe to drop the sensor for deployment. A possible network deployment method using UAV was experimented in [4].

In this paper, mobile access coordinated wireless sensor networks (MC-WSN) architecture is considered for energy-efficient, reliable, and time-sensitive information exchange. In MC-WSN, the whole network is divided into cells, each is covered by one MA. The MAs coordinate the network through deploying, replacing and recharging nodes. They are also responsible for enhancing the network security, by detecting compromised nodes then replacing them [5]. Data transmission from sensor nodes to the MA goes through simple routing with the cluster heads along a ring or a powerful center cluster head located at the middle of each cell. Based on active network deployment and topology design, the number of hops from any sensor to the MA is minimized and limited to a pre-specified number. Unlike in SENMA, the delay in MC-WSN depends on the number of hops and the electromagnetic wave speed, and is independent of the physical speed of the MA. For MC-WSN, the energy consumption at the individual sensors is mainly determined by the distance from the nearest cluster head, which is one hop away, and is independent of the coverage area of the MA and the node density. We demonstrate the effectiveness of the proposed architecture through simulation examples, which show that the MC-WSN architecture achieves higher energy-efficiency and orders of magnitude lower delay over SENMA, especially for large-scale networks.

## II. REVISIT THE SENMA SYSTEM

To reduce the routing burden on individual sensors, SENMA networks utilize mobile access points to collect the sensing reports from all sensors nodes [1]. The access point traverses the network at a height $H_S$ broadcasting beacon signals at random locations. The coverage area of the access point is modeled as a circle of radius $r$. The access point activates sensors within its coverage area, and each time only a single sensor responds to the beacon message by reporting its sensing information.

In SENMA, since sensors communicate directly to the mobile access point without any routing, the energy consumption at the individual sensors is significantly reduced over ad-hoc networks [1]. For this to happen, the mobile access point needs to traverse its footprint exhaustively to cover all sensors, resulting in a very long mobile access trajectory and consequently

978-1-4673-3122-7/13/$31.00 ©2013 IEEE

huge delay. The delay depends on the physical speed of the MA and the length of the MA trajectory, which would increase significantly as the network size increases. Thus, SENMA could be undesirable for time-sensitive applications. Motivated by this observation, we propose a mobile access coordinated wireless sensor networks architecture.

## III. THE PROPOSED MOBILE ACCESS COORDINATED WIRELESS SENSOR NETWORK (MC-WSN)

In this section, we describe the proposed MC-WSN architecture that aims at providing reliable, energy-efficient and scalable network structure for prolonged-network lifetime and time-sensitive data exchange.

We assume the network is divided into hexagonally shaped cells, with sides of length $d$. Each cell contains a single powerful mobile access point (MA) and $K_{SN}$ uniformly deployed sensor nodes (SNs) that are arranged into $K_{CH}$ clusters, each is of radius $R_{CH}$. Each cluster is managed by a cluster head (CH), to which all the cluster members report their data. CHs then route the data to the MA. A powerful center cluster head (CCH) is employed in the middle of each cell. The CCH can establish direct communication with the MA as long as it is inside the cell. After receiving the data of the sensors, the MA delivers it to the Base Station (BS), which in turn makes the final decisions. To improve the network reliability, efficiency and scalability, multiple BSs can be employed. The overall network architecture is illustrated in Figure 1.

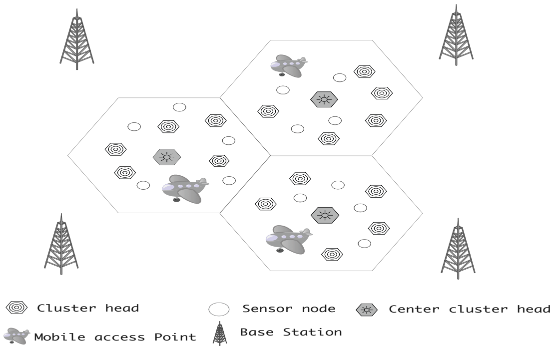

Fig. 1. Proposed MC-WSN architecture.

In the proposed MC-WSN architecture, the MA coordinates the sensor network and resolves the node deployment issue as well as the energy consumption problem of wireless sensor networks. More specifically, the MAs are responsible for (i) deploying nodes, (ii) replacing and recharging nodes, (iii) detecting malicious sensors, then removing and replacing them, (iv) collecting the information from sensors and delivering it to the BS.

When an MA needs to be recharged or reloaded, it sends a request to the MA base. The base will send a new MA to the cell, and the old MA will be taken back to the base for maintenance services. The MAs can move on the ground, and can also fly. Each MA traverses its cell mainly for removing the malicious nodes and replacing or recharging low-energy sensor nodes and cluster heads. It moves physically for data collection only in the case when the routing paths do not work. Otherwise, for security reasons, it stays at a random location on a circular path of a radius $R_t$ and at an angle $\phi$ from the CCH as shown in Figure 2. $\phi$ is uniformly distributed with PDF $f_\phi(\phi) = \frac{1}{2\pi}$. The CHs along the circular path forms a ring, through which the data can be delivered to the MA. The ring is designed such that there is at least one CH on it can communicate directly with the MA, which we refer to as the RCH. This should be the one nearest to the MA location. Note that, since the MA moves randomly over the ring, the RCH is not fixed. It is also noted that the ring may not be a strict circle, and it depends on the coverage area of the MA.

Data transmission from any SN to the MA goes through simple routing, either with the CCH or the RCH. Let the communication range of each sensor node be $r_c$. SNs only communicate with their corresponding CH, which then route the data to the MA. CHs have larger storage capacity and longer communication range than SNs.

To minimize the delay in data transmission from the sensors to the MA, the number of hops needed in routing should be minimized. Therefore, we consider dividing the CHs in the cell into two groups based on their location. The first group contains CHs within the area of radius $R_o$ from the CCH. While the second group contains all CHs located outside the radius $R_o$, where $R_o < R_t$. CHs in the first group will mainly route their information to the MA through the CCH, which can deliver the data directly to the MA. While CHs in the second group route their information to the MA either directly or through the RCH. The latter case happens by first routing the data to the nearest CH on the ring, which then broadcasts the data in both directions along the ring until it reaches the RCH as shown in Figure 2. The RCH then deliver the data to the MA. To minimize the number of hops, if a CHs in the second group is very far from RCH, it can directly forwards its data to the CCH, as will be illustrated in Section V.

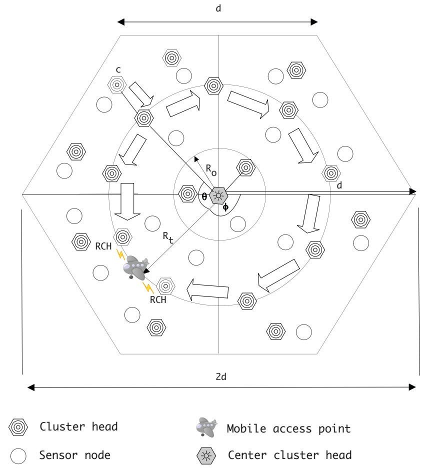

Fig. 2. The topology used in the MC-WSN architecture. Here CH c has a packet to deliver to the MA.

In the architecture design, we limit the average number of hops from any SN to its corresponding CH to $N_1$, and limit the average number of hops from any CH to the MA to $N_2$, where $N_1$ and $N_2$ are pre-specified numbers. $N_1$ is controlled through active network deployment, while $N_2$ is controlled through the network topology design (i.e. select the ring radius $R_t$ and the radius $R_o$).

The main features of the MC-WSN architecture are:

- *Resolve the network deployment problem and actively prolong the network lifetime* The proposed MC-WSN allows the MAs to manage the deployment of SNs and CHs. That is, the MA can add more nodes, relocate or replace exiting nodes. In addition, it can recharge or replace low energy nodes. When a node has low remaining energy, it sends a control message to the MA notifying it with its energy level. The MA can then make the decision to replace the node or recharge it. Being coordinated by the MA, the MC-WSN architecture resolves the network deployment issue and can actively prolong the network lifetime.
- *Minimize the delay* Unlike in SENMA, where the data collection delay depends on the physical velocity of the MA, in MC-WSN the delay depends on the number of hops and the electromagnetic wave speed, and is independent of the physical speed of the MA. Therefore, the delay is significantly lower than that in SENMA. The delay is further reduced by minimizing the number of hops required to reach the MA; this is achieved through network topology design and active network deployment.
- *Provide high energy efficiency* The SNs have the most limited resources in wireless sensor networks. In the proposed MC-WSN, SNs only communicate with their nearest CHs, and are not involved in any inter-cluster routing. Also, in contrast to SENMA, SNs in MC-WSN do not need to receive the beacon signal from the MA.
- *Enhance network security* The MAs can detect malicious SNs and CHs and replace them [5]. It is difficult to get the MA itself compromised or destroyed, since it is much more powerful than other network nodes, and it moves randomly in the network where its location can be kept private [6].
- *Enhance network resilience, reliability and scalability:* The MC-WSN is a self-healing architecture, where the CCH and RCH represent two options for relaying the data to the MA. Each option can act as an alternative for the other. In the case when the routing paths do not work, the MA can traverse its cell for data collection. Overall, MC-WSN is a resilient, reliable and scalable architecture.

*Discussions on Feasibility:* Sensor nodes and MAs deployment in different cells is possible through the UAV technology. A helicopter, or a larger unmanned aerial vehicle, can deploy the MAs in the network, and can replace existing MAs when they are out of energy. The sensor deployment is initiated by the UAV and then tuned by the MA.

## IV. NETWORK OPERATIONS

In this section, we illustrate the main network procedures used in MC-WSN.

### A. Network Set-Up

We assume that the CHs and the MAs are equipped with Global Positioning System (GPS) to obtain their location information. The network set-up is established through the following steps:

1) *Cluster formation:* All CHs broadcast *Hello* messages containing their IDs and locations. Each SN detects it nearest CH, to which it sends a Request to Join $(RTJ)$. Upon reception of $RTJ$, CH replies with Confirm to Join $(CTJ)$.
2) *Ring set-up:* The MA traverses the cell along a circular ring of radius $R_t$ broadcasting *Start* messages to the CHs in its coverage area. Denote the set of CHs that are along the ring and within the MA coverage area as $\chi$. All the CHs in $\chi$ receive the *Start* message, and reply to the MA with an *ACK*.
3) *Discover links to the ring:* broadcast *InitCH* message to all their neighboring CHs. The *InitCH* message includes the ID and location of the sender CH. When a CH receives the *InitCH*, it will in turn broadcast *InitCH* to its neighbors. This happens until all CHs receive at least a single *InitCH* message. Confirmation is made backward through the same links.
4) *Discover links to the CCH:* CCH also broadcasts a *Reference* signal to all its neighboring CHs. The *Reference* signal is forwarded by CHs, using the same manner discussed above, until it reaches the CHs on the ring.
5) *Establish the links to the ring or the CCH:* CHs then establish connections with the CCH and/or the closest CH on the ring by sending Request to Connect $(RTC)$ message. The process is completed when the intended receiver replies with Confirm to Connect $(CTC)$.

### B. Sensing and Collecting

The sensing and collecting stage is performed periodically, where the individual sensors monitor the environment and report their information to the CHs. When TDMA is used within clusters, each SN reports to its corresponding CH a *data* message in its allotted time slot. In order to minimize the interference between clusters (inter-cluster interference), Direct Sequence Spread Spectrum (DSSS) can be used, where the nodes of the different clusters use different spreading codes [7]. Also, data transmissions from SNs to CHs, between CHs, from CHs to the MA, and from the CCH to the MA are made over different frequencies to avoid interference between the different communication links.

CHs route the sensing information to the MA through their established links with the CCH or any node in $\chi$. When the MA visits a region, it sends a *beacon* signal to the CHs within its coverage area. If a CH receives the *beacon* signal, then it can respond directly by sending its data to the MA. If the data is received correctly, the MA responds with an ACK. It is noted that the data a CH sends to the MA can be information from its own cluster members, or from other clusters that relay their data through it.

### *C. Malicious Node Detection*

When the MA receives data from a node, it first authenticates the source and checks its identity. If the node passes the authentication procedure, its data would be used in the final decision making process. Some authenticated sensors can be compromised and may report fictitious data. This is known as Byzantine attacks [5]. The MA should be able to detect these malicious nodes and avoid their harmful effect. One way to detect compromised nodes is to use a reliable data fusion scheme [5], on the information collected from many sensors, and obtain the final decision. The MA monitors the reports of each individual node and compares it with the final decision obtained by the data fusion. Based on the observations over several sensing periods, the malicious nodes can be detected and removed.

## V. THE NETWORK TOPOLOGY DESIGN

In this section, we obtain the optimal radius $R_o$ and the ring radius $R_t$ that minimize the required number of hops from any CH to the MA. Define $\theta$ as the smaller angle between the MA position and the CH on the ring that first received the data; the PDF of $\theta$ is $f_\theta(\theta) = \frac{1}{\pi}$. Assume that two cluster heads separated by a distance $2R_{CH}$ can communicate directly. Then, for a given $\theta$, routing along the ring requires approximately $\left\lceil \frac{\theta R_t}{2R_{CH}} \right\rceil$ hops to reach the RCH. While, the routing from the ring to the CCH requires $\left\lceil \frac{R_t}{2R_{CH}} \right\rceil$ hops. Therefore, to minimize the number of hops for nodes outside the ring, the routing over the ring is made under the condition that $\theta < 1$, i.e., $\theta < 57.3^\circ$. If this condition is not satisfied, nodes reach the MA mainly through the CCH. Nodes in the region between $R_o$ and $R_t$ route their data through the ring if $\frac{\theta R_t}{2R_{CH}} + \frac{R_t - x}{2R_{CH}} < \frac{x}{2R_{CH}}$. That is, if $\theta < \frac{2x}{R_t} - 1$, the nodes at distance $R_o \leq x < R_t$ route their data to the RCH. Otherwise, they route the data to the $CCH$. We assume that CHs along the ring can estimate $\theta$ from the beacon signal they receive. The RCH notifies the nodes in the region between $R_o$ and $R_t$ that are connected to it. If the nodes in this region do not receive a notification from the RCH, then they forward their data to the CCH.

Let $N_{hops}$ be the average number of hops required to route the data from any CH in the network to the CH that can establish direct communication with the MA, i.e., the CCH or the RCH. Note that the number of hops to reach the MA is $N_2 = N_{hops} + 1$. $N_{hops}$ is given by:

$$\begin{aligned} N_{hops} \;=\; & \frac{1}{2R_{CH}} \left[ \int_0^{R_o} x f_X(x) dx \right. \\ & + \int_{x=R_o}^{R_t} \int_{\theta=\frac{2x}{R_t}-1}^{\pi} x f_X(x) f_\theta(\theta) d\theta dx \\ & + \int_{x=R_o}^{R_t} \int_{\theta=0}^{\frac{2x}{R_t}-1} \left(R_t - x + \theta R_t\right) f_X(x) f_\theta(\theta) d\theta dx \\ & + \int_{x=R_t}^{d} \int_{\theta=1}^{\pi} x f_X(x) f_\theta(\theta) d\theta dx \\ & \left. + \int_{x=R_t}^{d} \int_{\theta=0}^{1} \left(x - R_t + \theta R_t\right) f_X(x) f_\theta(\theta) d\theta dx \right], (1) \end{aligned}$$

where $x$ is the distance from any CH to the center of the cell, $f_X(x)$ is the PDF of $x$ and can be approximated by $f_X(x) = \frac{2x}{d^2}$ assuming that the CHs are uniformly distributed in a circle of radius $d$.

By setting $\frac{\partial N_{hops}}{\partial R_o} = 0$, we obtain the optimal $R_o = 0.5\ R_t$. Then, we substitute in (1) with the optimal $R_o$, and obtain the optimal $R_t$ by setting $\frac{\partial N_{hops}}{\partial R_t} = 0$. We get $R_t = 0.686\ d$; it then follows that $R_o = 0.343\ d$.

***Proposition**: To minimize the data collection delay in MC-WSN, the following conditions should be met. (1) The CHs within a distance $R_o = 0.343\ d$ from the center of the cell deliver their data to the MA through the CCH. (2) Nodes at a distance $x$ from CCH, where $R_o \leq x < R_t$, deliver their data to the MA through the ring if $\theta < \frac{2x}{R_t} - 1$, or through the CCH if $\theta > \frac{2x}{R_t} - 1$. (3) Other nodes at a distance $x \geq R_t$ from the CCH , deliver their data to the MA through the ring if $\theta < 1$, or through the CCH if $\theta > 1$. The ring radius is $R_t = 0.686\ d$.*

The delay is proportional to the number of hops required for routing the data to the MA. The average distance traveled corresponding to $N_{hops}$ is $2R_{CH}N_{hops}$; therefore, the delay in packet delivery is $D_M \propto \frac{2R_{CH}N_{hops}}{V_{EM}}$, where $V_{EM} = 3 \times 10^8\ m/s$ is the electromagnetic wave (EM) propagation speed.

## VI. NUMERICAL RESULTS

**Example 1: Delay comparisons** For delay calculations, we assume that there are no collisions or retransmissions. We also assume that each SN reaches its nearest CH in one hop, which can be ensured with the active network deployment, and the number of hops from the RCH or CCH to the MA is one. Therefore, we use the number of hops to reach the RCH or the CCH as an indication of the delay.

To show the effectiveness of our proposed architecture, we compare two topologies: (a) Topology 1: all nodes in the cell use the CCH to deliver their data to the MA. (b) Topology 2: both the CCH and the RCH are employed to deliver the data to the MA. For topology 1, let $N_{hops,1}$ be the average number of hops for a CH to reach the CCH. Then, $N_{hops,1} = \int_0^d \frac{x}{2R_{CH}} f_X(x) dx = \frac{d}{3R_{CH}}$. For topology 2, the number of hops is obtained using (1). By substituting with $R_t = 0.686\ d$, we get $N_{hops,2} = N_{hops} = 0.297 \frac{d}{R_{CH}}$. Comparing $N_{hops,2}$ with $N_{hops,1}$, it can be seen that lower delay can be achieved with the proposed topology (topology 2). This is further illustrated in Figure 3, where the number of hops is plotted versus $d$ for both topologies.

The delay in data delivery ($D_M$) can be expressed as: $D_M = C_1 \frac{d}{V_{EM}}$ , where $C_1$ is a constant. In SENMA, the SNs wait for the MA visit to report their data; hence, the delay depends on the velocity of the MA, as well as the cell size; that is, the average delay for a node to report its data to the MA in SENMA is $D_S = C_2 \frac{d^2}{V_{MA}}$ [1], where $V_{MA}$ is the MA speed and $C_2$ is a constant. Therefore, we have $\frac{D_S}{D_M} = Cd\frac{V_{EM}}{V_{MA}}$, where $C$ is a constant. This implies that the proposed MC-WSN architecture could result in several orders of magnitude lower delay over SENMA. The delay reduction is proportional to the ratio between the speed of light (EM speed) and the physical speed of the MA. Table I shows the delay ratio $\frac{D_S}{D_M}$ for different cell sizes.

TABLE I
DELAY COMPARISON WITH $V_{MA} = 30\ m/s$.

| Cell edge length (m): $d$ | 100 | 1000 |
|---|---|---|
| Delay ratio: $\frac{D_S}{D_M}$ | $\propto 10^9$ | $\propto 10^{10}$ |

$D_S$: Average delay in SENMA, $D_M$: Average delay in MC-WSN.

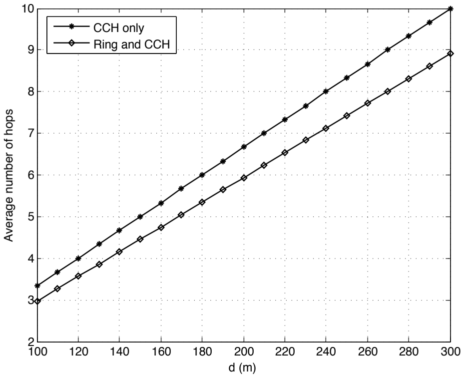

Fig. 3. The average number of hops in the cases when the communication with the MA is established through the CCH only ($N_{hops,1}$), and both the CCH and the ring ($N_{hops,2}$) . Here we use $R_{CH} = 10m$.

**Example 2: Energy efficiency** We focus on the energy dissipated in the individual SNs, since they have the most limited resources. We use the circuitry radio energy dissipation model to evaluate the energy efficiency [7]. We assume that the radius of the cluster is $R_{CH} = r_c$. Let $E_{tx}$ and $E_{rx}$ be the energy dissipated in the transmitter and receiver electronics of the SNs, respectively. Then, in MC-WSN, the maximum energy dissipated in SN to transmit a bit to the CH is $E_{SN,M} = E_{tx} + \epsilon_{pa} r_c^{\gamma}\ (J/bit)$, where $\epsilon_{pa}$ is the energy consumed by the power amplifier, $\gamma$ is the path loss exponent.

In SENMA, each SN must first receive a beacon signal from the MA in order to report its data. Therefore, the energy dissipated by a node to report a single bit to the MA is $E_{SN,S} = E_{tx} + \epsilon_{pa} H_S^{\gamma} + E_{rx} \pi r^2 \frac{K_{SN}}{A_c}$ [1], where $A_c$ is the area of the cell. Figure 4 shows $E_{SN,M}$ and $E_{SN,S}$ as the number of sensor nodes increases. It can be seen from the figure that the MC-WSN is significantly more energy-efficient than SENMA, especially when the density of the sensors increases.

It should be noted that energy dissipation in the CHs and MAs are ignored here. However, if their energy dissipation is taken into account, the MC-WSN would still be more efficient than SENMA architecture; since in SENMA, the MA is assumed to traverse the network continuously leading to a very high energy consumption.

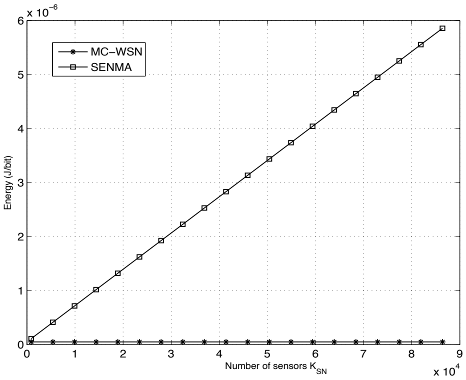

Fig. 4. The energy dissipation (J/bit) vs. the number of SNs in the MC-WSN and SENMA networks, when $d = 100m$, $r_c = r = 10m$, $H_S = 10m$, $\gamma = 2$, $E_{tx} = E_{rx} = 50\ pJ/bit$ and $\epsilon = 10\ pJ/bit/m^2$

## VII. CONCLUSIONS

In this paper, we proposed a reliable and energy-efficient architecture design for mobile access coordinated wireless sensor networks (MC-WSN). In the proposed architecture, the network exploits the mobile access points to actively deploy nodes, perform data collection, detect malicious sensors and enhance the network security. Not only does the MC-WSN resolve the network deployment problem, but it also prolongs the network lifetime actively and provides an efficient framework for time-sensitive information exchange. Simulation results showed that the proposed MC-WSN architecture can achieve higher energy efficiency and several orders of magnitude lower delay over SENMA. The gains achieved by the proposed architecture increase as the network size increases.

## REFERENCES

[1] G. Mergen, Z. Qing, and L. Tong, “Sensor networks with mobile access: Energy and capacity considerations,” *IEEE Transactions on Communications,*, vol. 54, no. 11, pp. 2033–2044, Nov. 2006.

[2] A. Poornima and B. Amberker, “Agent based secure data collection in heterogeneous sensor networks,” *2010 Second International Conference on Machine Learning and Computing (ICMLC)*, pp. 116–120, Feb. 2010.

[3] I. Maza, F. Caballero, J. Capitan, J. Martinez-de Dios, and A. Ollero, “A distributed architecture for a robotic platform with aerial sensor transportation and self-deployment capabilities,” *Journal of Field Robotics*, vol. 28, no. 3, pp. 303–328, 2011. [Online]. Available: http://dx.doi.org/10.1002/rob.20383

[4] P. Corke, S. Hrabar, R. Peterson, D. Rus, S. Saripalli, and G. Sukhatme, “Autonomous deployment and repair of a sensor network using an unmanned aerial vehicle,” *IEEE International Conference on Robotics and Automation, ICRA ’04*, vol. 4, pp. 3602 – 3608 Vol.4, 26-May 1, 2004.

[5] M. Abdelhakim, L. Lightfoot, and T. Li, “Reliable data fusion in wireless sensor networks under byzantine attacks,” *IEEE Military Communications Conference, MILCOM*, Nov. 2011.

[6] J. Ren, Y. Li, and T. Li, “Spm: Source privacy for mobile ad hoc networks,” *EURASIP J. Wireless Comm. and Networking*, 2010.

[7] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “An application-specific protocol architecture for wireless microsensor networks,” *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660 – 670, Oct. 2002.