IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. VII (May – Jun. 2015), PP 09-15
www.iosrjournals.org

Security based Clock Synchronization technique in Wireless Sensor Network for Event Driven Measurement Applications

Mrs .Mary Cherian[1,] Latha M[2]
[1,]Associate Professor, Department Of CSE [2.] Student of M.Tech CSE
Dr. Ambedkar Institute of Technology, Bangalore

Abstract: *In this paper, secure based novel clock synchronization in wireless sensor network for event driven measurement application is proposed with security. The main objectives are 1) To provide high accuracy in the area where an event is detected 2) To ensure long network lifetime 3) To ensure security based packet transmission. The complexity of a problem arises from first two properties that usually in clash. To increase the synchronization accuracy, the nodes are required to transfer synchronization packets at higher rate thus impacting the network lifetime. Vice versa to increase the lifetime of network, number of packet transfer around the nodes should be minimized, thus impacting the synchronization accuracy. A tradeoff can be accomplished by viewing that the packet rate need to be increased only for the part of the network surrounded by events as only those nodes requires high accuracy to collect data. In order to rectify an adversary who aims to tamper with the clock synchronization by intercepting messages, replying to intercept messages and revealing of secret keys, proper authentication needs to be given. Security is provided for packet transmission on a network, resilient to the aforementioned adversarial attacks. The simulation results show the accurate date and time of event occurrence.*

Keywords: *Clock synchronization, Security, Timestamp, wireless sensor network (WSN).*

I. Introduction

Wireless sensor networks (WSNs) are distributed networks of sensors, dedicated to closely observing real-world phenomena. Such sensors may be embedded in the environment or enabled with mobility; they can be deployed in inaccessible, dangerous, or hostile environments. The sensors collaborate with each other and form a communication network and gather wide range of information available in the environment. This will result in attaining a border picture of the environment. Applications using wireless sensor network include network localization [1]-[3] health care monitoring [4], flood detection [5], debris flow [6], landslide detection, natural disaster prevention, intrusion detection and so on.

Clock synchronization protocols for the rapidly emerging wireless sensor network are based on factors such as precision, accuracy, cost, and complexity. Synchronization protocols will guide designers in defining new protocols tailored to specific applications of sensor networks. Clock synchronization in wireless sensor networks requires newer and more robust approaches. As in sensor networks, correct clocks have arbitrary starting offsets and nondeterministic fluctuating skews. A thorough understanding of the challenges posed by wireless sensor networks is crucial for the successful design of synchronization protocols for such networks to perform event driven measurement applications. The main approach of this application is to maintain a long life time of nodes in wireless sensor networks and provide high accuracy and security around the nodes by authenticating the message that has to be passed.

In this paper a novel clock synchronization algorithm is proposed for measurement applications. The algorithm makes a tradeoff between network lifetime preservation and synchronization accuracy. High accuracy should be given around the nodes where events are detected. For an event driven measurement application synchronization protocol will selectively increase or decrease the packets rate of exchange based on the events that are present among the nodes, while rest of the area in a network maintains a low accuracy. The system strives to synchronize with system clock by monitoring the adversary. The security based algorithm is introduced that will identify intercept message sent by attackers. Secure synchronization protocol is proposed that mask attack by an adversary that aims to make the protocol give an erroneous output.

Therefore, the set of WSN nodes is logically divided into two subsets;

1. Improved synchronization subset (ISS), where the nodes that are detected with the event are ensured with ISS in which high accuracy is given to this particular area.
2. Default synchronization subset (DSS), where the nodes maintain a low accuracy in which no events are present in that particular area. The lifetime of a network can be increased with less energy consumption.

II. Related Work

Synchronization for WSN can be classified into two main types namely hierarchical and fully distributed. Algorithms used previously were organized into tree based structure where each node refers to its parent node, to compensate the clock skew and clock drift [8][9]. The significant restriction of this methodology is that, whenever the root or a parent node gets to be inaccessible, the related sub-tree looses synchronization until the system is redesigned. So to overcome this problem, network is organized into cluster based manner in which node synchronization is done in the same cluster. EL kheddiri [10] proposed to opt for a local master within each cluster. The local master is synchronized to accomplish a common sense of time. But in case of a failure of local master, cluster related to that network becomes unsynchronized.

In [11] to find energy consumption, sensors are grouped into clusters. Each cluster has a cluster head. Based on this communication among the nodes in the network is done, but finding an optimal probability of a cluster head was difficult.

Algorithms belonging to latter [12-15], are robust to node failures as a master node does not exist. On the contrary, the common sense of time is accomplished through local collaboration among the nodes.

In [13]-[17] algorithm based on consensus protocol is proposed. They can be classified on the basis of 1) the parameters object of the estimation and compensation 2) communication modalities synchronous or asynchronous.

In particular, in [13] Consensus approach is used to find clock offsets in sparely physical populated mobile adhoc networks. In [14] consensus approach is used to compensate the clock drift and skew for phase locked loops. In [15] a second order consensus approach is followed to compensate clock drift and clock offsets, but it requires pseudo synchronous communication among nodes. In [17] a novel synchronization algorithm is proposed to ensure good level of synchronization even in the occurrence of random bounded communication delay. In [7] and [18] simple algorithms have been introduced, where consensus algorithms are used in an energetically efficient way so as to obtain accurate synchronization only in selected area, while preserving global convergence property.

Comparing with existing synchronization schemes, the novel methods proposed are as follows,

- Improvement of the framework presented in [7], by proposing a new communication policy ISS (improved synchronization subset) that alerts if an event is present on a network.
- Extension of the single event scenario into multiple events scenario.
- Secure clock synchronization in sensor networks whereas packet transmission is done based on proper authentication.

III. Problem Statement

Consider a wireless sensor network (WSN) made out of N nodes with topology depicted by an undirected graph G ={V,E} with V=(1…N} the set of nodes representing the sensors and E={ i, j}is the set of edges that are portraying the point to point channel availability ,i.e., an edge(i , j) exists , if node i can transmit to node j. Note that since the network topology is undirected so the existence of the edge (i, j) suggests the existence of the edge (j,i). Let the neighborhood V_i of a node i be the set V_i ={ j : (i, j) ∈ E}, with |Vi| its cardinality. Further-more, indicate with t_k the moment when the kth communication on the WSN happens and $G(t_k)$ ={ V, $E(t_k)$} the possibly directed graph that portrays the communication at time t_k, i.e., (i, j) ∈ $E(t_k)$ if the node i sends data to the node j at time t_k. Clearly, $E(t_k) \subseteq E$ at each time step t_k.

Finally, denote as rooted graph, a graph that exists at least one node for which a path with any other node can be settled. Each node i is set up with a (local) hardware clock τ_i defined as

$$\tau_i(t) = \alpha_i t + \beta_i \qquad (1)$$

where α_i is the local clock frequency and β_i is the offset. Notably, the coefficients (α_i,β_i) contrast for each node to another node due to actual hardware components. Subsequently, a synchronization algorithm must be provided to keep a common notion of time, otherwise clocks might diverge with respect to the others.

The following components are necessary to build a framework.

1) The synchronization protocol - To keep a common notion of time among node clocks.
2) ISS algorithm - To build a unique ISS in updating the events.

IV. System Architecture

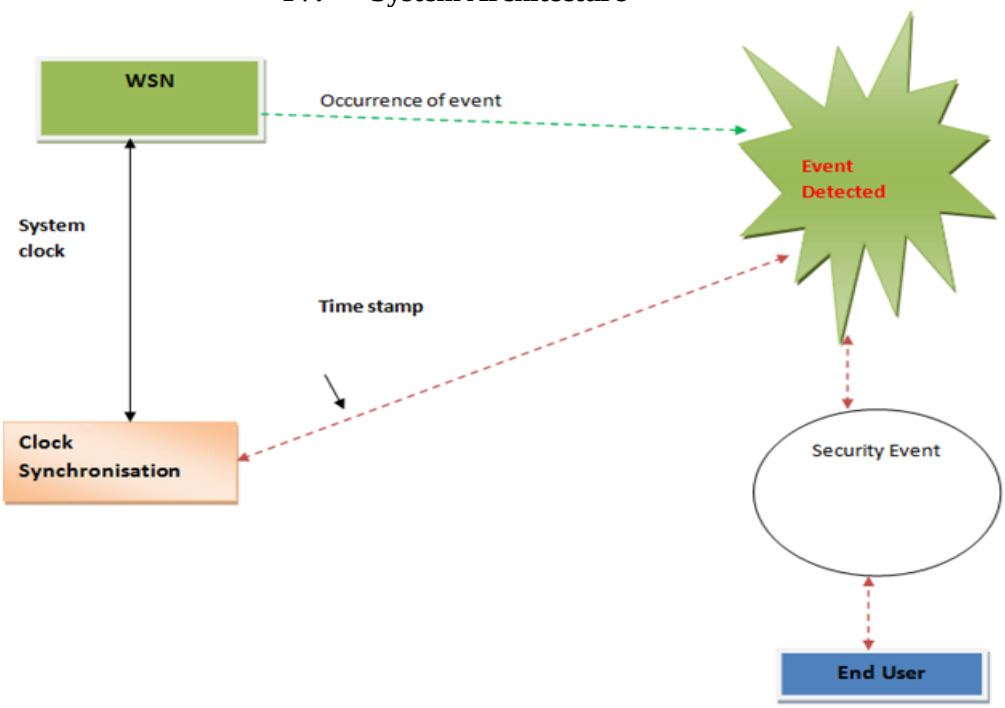

Figure 1 Design architecture.

As shown in Figure 1, the nodes are initialized in a network, based on the topological manner in which the nodes are positioned. If the events are detected on a network, then clock is synchronized to that particular event by taking system clock as a reference. The accurate time and date of the event is displayed. If the event is packet transmission, then the data should be authenticated. Security event is proposed for this purpose, as it saves the message from attackers.

V. Implementation

The ATS algorithm as well as the revised version of ATS can be implemented in an event-driven fashion, according to an asynchronous communication scheme. For packet transmission each node i sends packets when the software clock is such that there exists an integer m satisfying $\acute{r}_i(t) = t_i + mT_i$. In other words, the node i will send a packet periodically on the basis of its software clock with a synchronization period T_i and with an offset ti∈ (0, Ti).

A.ATS Algorithm

The ATS synchronization algorithm is based on the idea that each node regulates its own $\grave{\alpha}_i(t)$ and $\hat{o}_i(t)$ through local interactions with its neighbors. In particular, let t_k be the time when the node j sends a packet into the network. The packet contains the tuple $(id_j, \grave{\alpha}_j, \hat{o}_j, \tau_j)$ where id_j is an identifier of the jth node. $\grave{\alpha}_j = \grave{\alpha}_j(t_k)$ and $\hat{o}_j = \hat{o}_j(t_k)$ are the local clock corrections at time t_k and τ_j is the hardware timestamp of the packet, i.e., the value of the hardware clock in the moment the message is sent $\tau_j = \tau_j(t_k)$. When a node i receives the packet, it first stores the current value of its hardware local clock in a variable τ_{ij}. Assuming the transmission and time stamping operations instantaneous, $\tau_{ij} = \tau_i(t_k)$. Node i executes the local synchronization procedure that consist of three steps.

1) Relative Drift Estimation: The ith node computes the relative drift estimation $\alpha_{ij}(t^+_k)$ analyzing τi and τj in two different moments and calculating the relative frequencies. To this end, each node i must store two variables τ^{old}_j, τ^{old}_{ij} for each neighbor j in an internal structure. It follows:

$$\alpha_{ij}(t^+_k) = \frac{\alpha_j}{\alpha_i} = (\tau_j - \tau^{old}_j) / (\tau_{ij} - \tau^{old}_{ij}) \quad (2)$$

where α_i, α_j are the real clock frequencies for the nodes i and j, respectively. τ_j and τ_{ij} are stored into τ^{old}_j and τ^{old}_{ij} after the update.

2) Drift Compensation: $\grave{\alpha}_i$ is updated on the basis of $\alpha_{ij}(t^+_k)$ as follows:

$$\grave{\alpha}_i(t^+_k) = \rho_v \, \grave{\alpha}_i(t_k)^+ \, (1-\rho_v) / \alpha_{ij}(t^+_k) \, \grave{\alpha}_j(t_k) \quad (3)$$

3) Offset Compensation: $\hat{o}_i$ is updated as follows:

$\hat{o}_i(t^+_k)=\hat{o}_i(t_k) + (1 - \rho_o)(\acute{r}_j(t_k) - \acute{r}_i(t_k))$ (4)

where ρ_v and ρ_o are design parameters that can be set between 0 and 1. The correction parameters are usually initialized at $\grave{\alpha}_i$ =1, $\hat{o}_i$ =0, with i =1,...,N. Note that (2) and (3) can be performed only if at least one message from node j has been previously received.

B. Revised ATS

In this paper, the ATS algorithm is modified by replacing the offset compensation term (4) with the following one:

$\hat{o}_i(t^+_k) = \hat{o}_i(t_k) + (1 - \rho_o)(\acute{r}_j(t_k) - \acute{r}_i(t_k)) - \grave{\alpha}_i(t_k)\tau_i(t_k)$ (5)

where $\grave{\alpha}_i(t_k) = (\grave{\alpha}_i(t^+_k) - \grave{\alpha}_i(t_k))$. The importance of this improvement is that the additional correction term prevents the software clock time $\acute{r}_i(t)$ being over compensated due to changes of the α_i values.

C. Time stamp accuracy

In this section, we note down the timestamp of the events that is detected on the network. Therefore, it is sufficient to access the system clock counter during the detection of event in a network. Accuracy is maintained while event is detected. Meanwhile the system clock, notes down the time and date of the event occurred. It displays the system time; not the simulation time of the network simulator.

D. Security based packet transmission

A sensor network is a special type of network. It shares some commonalities with a typical computer network, but also poses unique requirements of its own. Proper authentication should be provided in these cases. If the data needs to be sent from one node to another node the data should be authenticated with a secret key. The message that has been encrypted based on the secret key ensures that the message is not hacked by attackers. If anyone is trying to intercept the message using secret key, it can be identified by system clock which notes down the time and date through clock synchronization technique.

E. ISS connector algorithm (improved synchronization subset)

In this module, multiple events occurrence in the network is identified by a unique component ISS (improved synchronization subset). In particular, if the events are detected in WSN, those nodes are set to be in alert mode so that data transmitting through those nodes requires high accuracy. Accuracy should be maintained in that particular region, where the rest of the nodes maintain low accuracy, i.e. DSS (default synchronization subset). The nodes with low accuracy are said to be in quiet state. The nodes which are given high accuracy to transmit data are said to be in alert state.

F. Flowchart

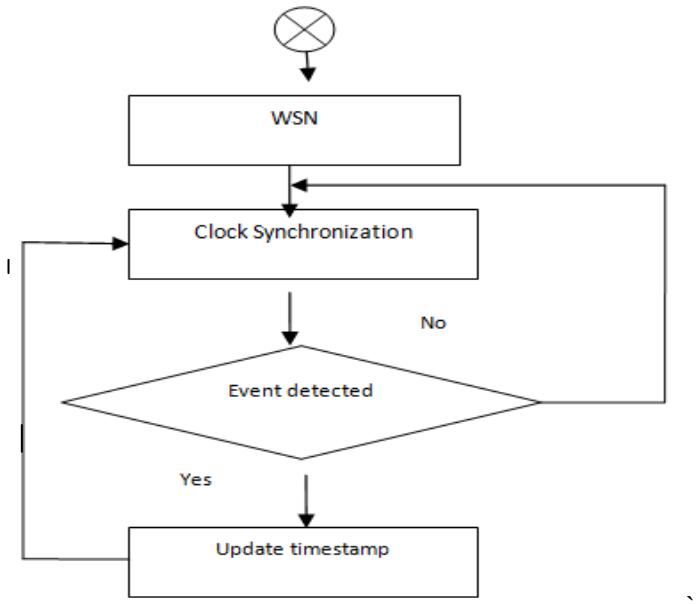

Figure 2: flowchart

Figure 2, explains the overall flow diagram of the process. The nodes in the wireless sensor network (WSN) are initialized and communication with the neighboring nodes is done. Clock synchronization is done based on algorithm synchronization protocol, which maintains a common sense of time of each event that is detected. Let the event be node neighboring calculation, if the event is detected then it updates the timestamp, and suitable time and date are displayed on that particular event.

G. Data flow diagram

Level 0

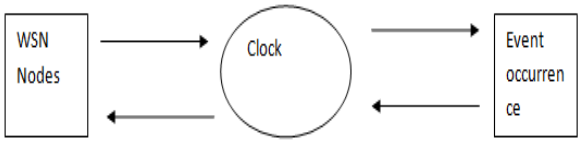

Figure 3: Level 0 Data flow diagram

In Figure 3, level 0, the nodes in the wireless sensor network (WSN) after initialization are connected for clock synchronization. If the event is detected on network then it returns a result as the event occurred.

Level 1

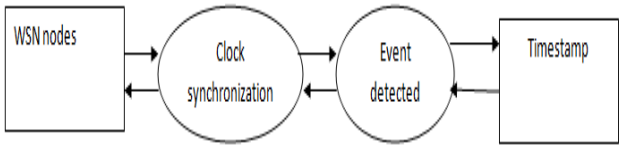

Figure 4: Level 1 Data flow diagram

In Figure 4, level 1, if an event is detected on a wireless sensor network (WSN), the clock synchronizes to the event occurrence and the time stamp will display a date and time of that particular event detected in the network.

VI. Results And Analysis

In this section the experiments conducted with NS2 indicate the clock synchronization technique in WSN for event driven application. As the event occurs in a network, clock synchronizes to the event and updates the time and date of the occurrence of an event. Keeping system as hardware equipment, the date and time are displayed. It maintains the long network lifetime by consuming less energy during packet transmission. Here we consider 100 nodes deployed in the area of 800*800 and initial energy is set to 100J.

Snapshots:

As the event is detected on a network, in the log file the accurate time and date of event occurrence is displayed.

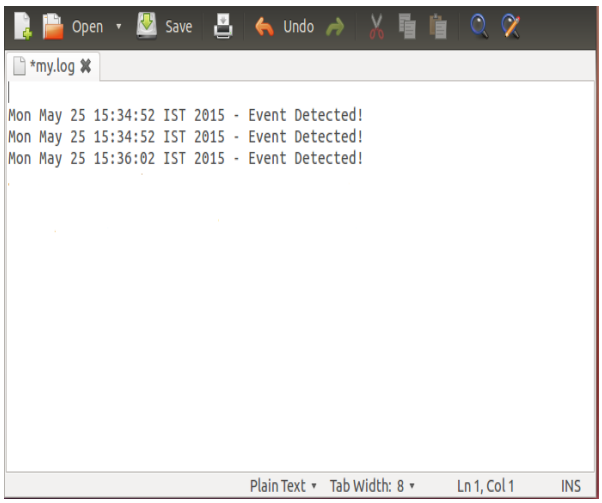

Figure 5: representing of time and date in log file on the event detection

Following graphs represent the throughput, delay and packet delivery ratio. These parameters indicate the good performance of the algorithm.

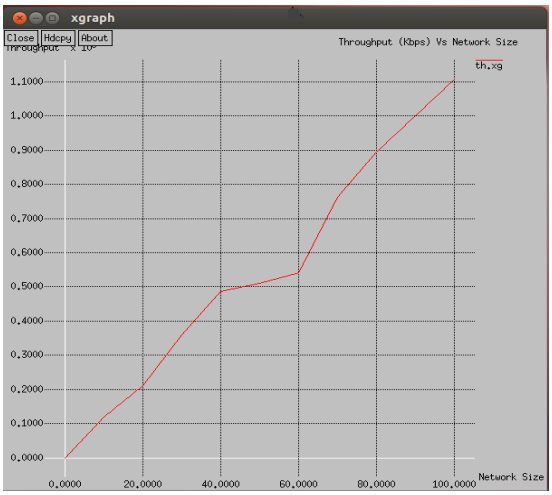

Figure 6: Throughput (100 nodes)

The above graph represents the throughput for 100 nodes. The throughput is measured in kilo bytes per unit second (kbps)
Average Throughput [kbps] =968.09
Start time=2.01 stop time=74.70

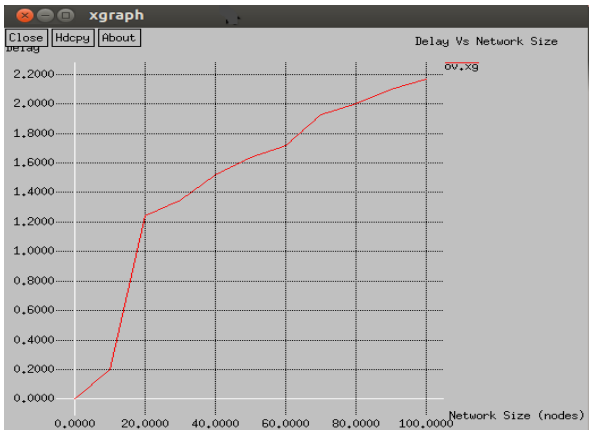

Figure 7: delay (100 nodes)

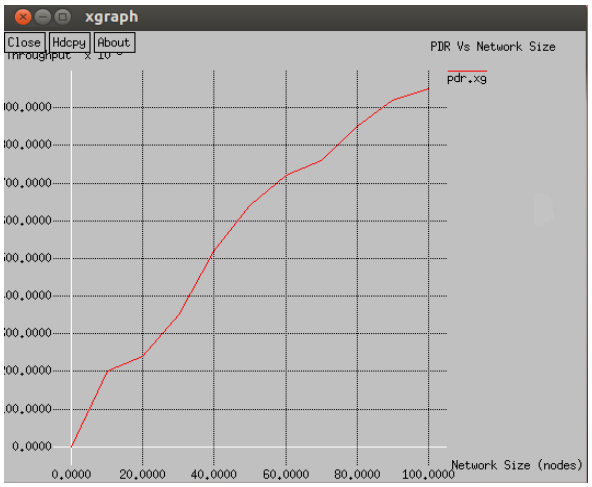

Figure 8: packet delivery ratio (PDR)

The above graph represents packet delivery ratio for 100 nodes, deployed in a network.

VII. Conclusion

In this paper, secure clock synchronization in WSN event driven measurement applications is proposed. The proposed algorithm represents a tradeoff between synchronization accuracy and network lifetime preservation and also security are maintained so that no one can hack the messages while packet transmission. Attacks can be prevented by authenticating the message. Experimental results confirm the accurate date and time of the event occurrence.

References

[1]. A. Colombo, D. Fontanelli, D. Macii, and L. Palopoli, "Flexible indoor localization and tracking based on a wearable platform and sensor data fusion," IEEE Trans. Instrum. Meas., doi: 10.1109/TIM.2013.2283546.

[2]. A. Gasparri and F. Pascucci, "An interlaced extended information filter for self-localization in sensor networks," IEEE Trans. Mobile Comput., vol. 9, no. 10, pp. 1491–1504, Oct. 2010.

[3]. B. Li, Y. He, F. Guo, and L. Zuo, "A novel localization algorithm based on isomap and partial least squares for wireless sensor networks," IEEE Trans. Instrum. Meas., vol. 62, no. 2, pp. 304–314, Feb. 2013.

[4]. L. Fanucci, S. Saponara, T. Bacchillone, M. Donati, P. Barba, I. Sanchez-Tato, et al., "Sensing devices and sensor signal processing for remote monitoring of vital signs in CHF patients," IEEE Trans. Instrum. Meas., vol. 62, no. 3, pp. 553–569, Mar. 2013.

[5]. A. Araujo, J. Garcia-Palacios, J. Blesa, F. Tirado, E. Romero, A. Samartin, et al., "Wireless measurement system for structural health monitoring with high time-synchronization accuracy," IEEE Trans. Instrum. Meas., vol. 61, no. 3, pp. 801–810, Mar. 2012.

[6]. L. H.-C. Lee, A. Banerjee, F. Yao-Min, L. Bing-Jean, and K. Chung-Ta, "Design of a multifunctional wireless sensor for in-situ monitoring of debris flows," IEEE Trans. Instrum. Meas., vol. 59, no. 11, pp. 2958–2967, Nov. 2010.

[7]. F. Lamonaca, E. Garone, D. Grimaldi, and A. Nastro, "Localized fine accuracy synchronization in wireless sensor network based on consensus approach," in Proc. IEEE Int. Instrum. Meas. Technol. Conf., May 2012, pp. 2802–2805.

[8]. S. Rahamatkar, "A Light Weight Time Synchronization Approach in Sensor Network: Tree Structured Referencing Time Synchronization Scheme," Saarbrücken, Germany: LAP Lambert Academic Publishing, 2012.

[9]. K.S. Yildirim and A. Kantarci, "Time synchronization based on slowflooding in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 244–253, Jan. 2014.

[10]. S. El Khediri, N. Nasr, A. Kachouri, and A. Wei, "Synchronization in wireless sensors networks using balanced clusters," in Proc. 6th Joint IFIP Wireless Mobile Netw. Conf., 2013, pp. 1–4.

[11]. Seema Bandyopadhyay and Edward J. Coyle School of Electrical and Computer Engineering "An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks", infocom 2003.ieee-infocom.org.

[12]. S. Merkel, C. W. Becker, and H. Schmeck, "Firefly-inspired synchronization for energy-efficient distance estimation in mobile ad-hoc networks," in Proc. IEEE 31st Int. Conf. Perform. Comput. Commun., Dec. 2012, pp. 205–214.

[13]. M. Sasabe and T. Takine, "Continuous-time analysis of the simple averaging scheme for global clock synchronization in sparsely populated MANETs," IEEE J. Sel. Areas Commun., vol. 31, no. 4, pp. 782–793, Apr. 2013.

[14]. O. Simeone and U. Spagnolini, "Distributed time synchronization in wireless sensor networks with coupled discrete-time oscillators," EURASIP J. Wireless Commun. Netw., vol. 7, no. 1, pp. 1–13, 2007.

[15]. R. Carli and S. Zampieri, "Networked clock synchronization based on second order linear consensus algorithms," in Proc. 49th IEEE Conf. Decision Control, Feb. 2010, pp. 20–28.

[16]. L. Schenato and F. Fiorentin, "Average timesynch: A consensus-based protocol for clock synchronization in wireless sensor networks," Automatica, vol. 47, no. 9, pp. 1878–1886, 2011.

[17]. E. Garone, A. Gasparri, and F. Lamonaca, "Clock synchronization for wireless sensor network with communication delay," in Proc. Amer. Control Conf., 2013, pp. 771–776.

[18]. F. Lamonaca, A. Gasparri, and E. Garone, "Wireless sensor networks clock synchronization with selective convergence rate," in Proc. Intell. Auto. Veh., 2013, pp. 146–151.

[19]. Francesco Lamonaca,Andrea Gasparri, Emanuele Garoneand Domenico Grimaldi, "Clock Synchronization in Wireless Sensor Network With Selective Convergence Rate for Event Driven Measurement Applications" IEEE Trans.Year: 2014, Volume: 63, Issue: 9 Pages: 2279 - 2287, DOI: 10.1109/TIM.2014.2304867.