Applying the Byzantine Agreement in Wireless Sensor Networks Based on Clustering

Pedram Kheirkhah Sangdeh[1], Mahtab Mirmohseni[2], Forough Poursabzi[3]

[1]School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran
Email: P_Kheirkhah@ut.ac.ir
[2]School of Electrical Engineering, Sharif University of Technology, Tehran, Iran
Email: Mirmohseni@sharif.edu
[3]School of Electrical and Computer Engineering, University of Colorado Boulder, Colorado, United States
Email: Forough.Poursabzisangdeh@colorado.edu

***Abstract*—Due to large communication overhead, applying Byzantine Agreement (BA) methods in Wireless Sensor Networks (WSNs) degrades their lifetime dramatically. Most of traditional proposed BAs assume that the processors are connected to unlimited resources of energy and the ideal links exist between them. A rough estimation about the required number of exchanged messages for decision in a network with n nodes is $O(n^2)$. Therefore, inefficient energy consumption becomes more challenging as network grows. Without any further actions, applying a BA method on a typical WSN is infeasible. In this paper, we propose a method for large scale WSNs which reaches agreement through two levels. In this method, we reduce the energy consumption of network through dividing the whole network to small groups of nodes by appropriate heuristic Leader First (LF) clustering; leading to fewer number of communications in shorter ranges. Our proposed method prolongs network lifetime, as well as maintaining reliability and robustness in a favorable range.**

I. Introduction

Over past decades, demands for Wireless Sensor Networks (WSNs) increased in both military and civil applications. A typical WSN consists of many tiny, cheap, battery powered, low end-processor sensors. Since these tiny sensors have limited non-rechargeable resource of energy, one of the most challenging issues in WSNs' territory is lifetime. Despite the wide spectrum of WSNs' applications, they are vulnerable to fail in their correct operations because of attackers, defective sensors, link failures and etc. An appropriate solution for preventing wrong decisions is making agreement amongst nodes. In agreement protocols, each node receives an input. Afterwards, the nodes exchange the received value and in the future rounds, they exchange all their received values at the previous round. This procedure continues until the agreement is reached. A common application of agreement is clock synchronization [1], [2]. Moreover, it can be utilized as a vital step before main task of network, for example, target detection. It is worth to mention that some secrecy protocols for WSNs also use agreement methods [3], [4].

Ramport *et al.* in [5] investigated Byzantine generals' problem and introduced one of the first agreement protocols for a network called Byzantine Agreement (BA). The term Byzantine is applied to the problem because they make no assumption on the behavior of faulty components. They also proved that reaching agreement is assured if the number of the defective processors in the network is less than $\lfloor \frac{n-1}{3} \rfloor$ within $\lfloor \frac{n-1}{3} \rfloor + 1$ rounds, where n denotes the number of processors. This scheme requires numerous and frequentative messages' communication that impose immense buffers and energy resources to nodes. In order to moderate the communication cost, some efforts have been done to achieve agreement in less rounds [6], [7]. These works assume benign conditions, which are proper only for wired networks since links' failure is one of the most common problems in the real world wireless communication medium due to fading, shadowing, pathloss, noise and interference. Thus, any agreement which fully trusts on communication links is not appropriate for applying on WSNs in most of practical cases. Furthermore, all of these works presume a fully-connected network through agreement procedure that is in contrast with inherit feature of WSNs, where sensors have a low cost communication module which is capable of communicating in short ranges. Hence, medium or large scale WSN networks are not fully-connected. Beside global agreement methods, there is another class of agreement approaches in which agreement can be achieved in a centralized manner. In centralized agreement protocols, each node sends its information to an aggregator node or a Cluster Head (CH). When aggregator node receives information from nodes, it makes decision and sends it to nodes. Although these methods reduce the communication cost to $O(n)$, they decline the robustness of system [8].

Motivated by these arguments, this paper mainly focuses on applying an global BA method in a WSN. In spite of major advances in representing heuristic and sophisticated agreement methods, there are huge obstacles toward the practical implementation of them in WSNs. This paper shows that with sacrificing a little bit of reliability, the communication cost can be decreased considerably. The key tool for balancing the trade-off between reliability and communication cost is a proper clustering method. Also, devising a compatible agreement paradigm is mandatory to maintain the reliability of system through clustering. In other words, as showed in this paper, a suitable combination of clustering and agreement leads to feasible implementation of BA in WSNs.

978-1-4799-1972-7/15/$31.00 ©2015 IEEE

The remaining of the paper is organized as follows: in the next section, the investigated problem is stated. In section III, the proposed clustering and agreement schemes are described in details. The simulation and the results are represented in section IV. Finally, the paper is concluded in section V.

II. Problem Statement

We consider a WSN with n nodes that requires a global BA on a detected event by a node in order to take proper decision about further actions. The nodes are deployed randomly on the sense field according to uniform probability distribution. Some works (see, for example [9]) assume possibility of adding replicas to network; however, we consider harsh environment in which replicas can not be added to the network. All nodes broadcast their messages and each of them is equipped with an omni-directional antenna. We presume defective or malicious nodes do not cooperate with each other and the final goal of the system is making decision about the validity of detection. Additionally, they do not care which nodes are defective, so oral messages are used during agreement and nodes are capable of recognizing the messages' sender. However, they cannot identify messages' original sources which is not needed in our case.

As we know, the communication cost of a global agreement is $O(n^2)$ [5]. The aim of our method is conducting an agreement scheme in a parallel manner at clusters. If we consider N_C clusters, the communication cost, denoted by T_{CC}, can be reduced as follows.

$$T_{CC}(n) = O(n_1^2) + O(n_2^2) + \ldots + O(n_{N_C}^2) + O(N_C^2); \quad (1)$$

$$n_1 + n_2 + \ldots + n_{N_C} = n; \quad (2)$$

where n_i denotes the number of nodes that pertains to i^{th} cluster and $O(N_C^2)$ is related to agreement at the second level, which is described in the next section. The main problem is minimizing T_{CC} under second equation's constraint and simultaneously reaching a reliable agreement in the considered WSN. In the following equations, CD stands for a tuple in which $CD(i) = n_i$.

$$CD_{opt} = \underset{n_1,\ldots,n_{N_C}}{\operatorname{argmin}} \{T_{CC}(n)\} \quad (3)$$

where CD_{opt} is the best clusters' distribution in terms of total communication cost. It is conspicuous that the CD_{opt} is as the following equation.

$$CD_{opt}(i) = \begin{cases} M+1 & \text{if } i \in \{1,\ldots r\}, \\ M & \text{if } i \in \{r+1,\ldots N_C\} \end{cases}; \quad (4a)$$

$$n = M \times N_C + r, \qquad M, r \in \mathbb{N}; \quad (4b)$$

where M is the integer quotient of n divided by N_C and r is its reminder. Owing to the symmetric conditions, all permutations of CD_{opt} are also the answers of equation (3). The equation (4) indicates that the clusters' sizes should be as close as possible in order to minimize the total communication cost of the agreement. Moreover, in our case, i.e. randomly deployed sensors with uniform distribution, number of sensors in a region is proportional to its area. Hence, it can be concluded that the proper clustering method must select CHs homogeneously over the sense field. A constant approach of clustering, for instance the one in [10], is inefficient in this case; because in each round, nodes of the largest cluster consume more power to communicate and they die earlier than the other nodes. As described in the next section, CHs participate in an agreement at the second level, so being a cluster head is an energy consuming role which must be considered in clustering.

In order to evaluate the performance of clustering, we introduce a variable X which is a suitable criterion to compare clustering methods in terms of homogeneity.

$$X = \sum_{i=1}^{r} (c_i - M - 1)^2 + \sum_{i=r+1}^{N_C} (c_i - M)^2; \quad (5)$$

where c_i stands for the size of i^{th} largest cluster. In other words, if we sort CD in decreasing order and show it by C, then X is the square of distance between C and CD_{opt}.

$$X = \sum_{i=1}^{N_C} (CD_{opt}(i) - C(i))^2; \quad (6)$$

To compare clustering methods, it is enough to run each one for several times and calculate X for each time. Any of them which leads to the least average of X is the superior one in terms of forming equal size clusters. Undoubtedly, any clustering method that permits to elect two close CHs may results in the sever inequality of cluster sizes. Moreover, omitting one of the two close CHs (see, for example [11]), to make homogeneity in CHs' distribution over sense field, imposes higher communication cost. It is more efficient to make CHs' distribution homogeneous before, but not after, selecting them.

At the agreement level, some considerations must be involved in the agreement and clustering mechanisms: *i*)- Whenever a global agreement makes decision at the presence of defective nodes and link failures, clustering method must not prevent network from reaching a successful agreement. *ii*)- Practically speaking, since it is possible that all nodes or all links of a region be defective or failed to successfully communicate, respectively, the clustering method should be capable of isolating the corruptness of links and nodes. For example, in the case of a moving or fixed obstacle, all the links of a region may go to shadow, i.e. shadowing phenomenon, or because of correlation between communication channels, most of the links in a region may fall to deep fade. Moreover, it is also possible that some nodes of a region be defected due to physical and environmental crashes. In conclusion, distribution of faulty nodes and links is not independent practically. Isolating feature makes reaching a successful agreement feasible for nodes; even if the number of faulty nodes and links are more than the maximum acceptable numbers of the original global agreement methods in some situations.

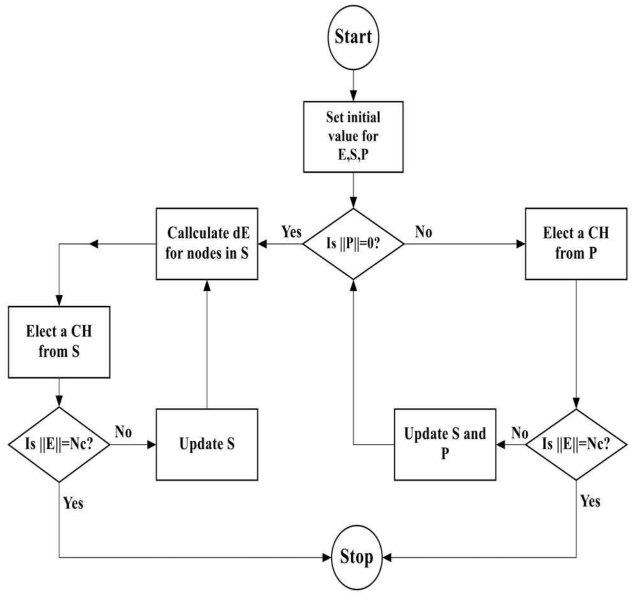

Fig. 1. Proposed method for cluster heads selection.

III. Proposed Method

A. Clustering

In Leader First (LF) clustering, CHs are selected in the first step and then other nodes are assigned to CHs to form clusters [12], [13]. In contrast to LF schemes, Cluster First (CF) approaches form clusters at first. Afterwards, the nodes of each cluster select their CH based on some metrics [10], [14], [15].

In our LF clustering approach, we assume a minimum distance between chosen CHs. In other words, when a CH is selected from some candidates, all nodes which are closer than the minimum allowable distance to the CH are ignored in the next CH's selection steps. This distance is pretested according to the final goal of clustering which is stated in the previous section.

$$s_c = \frac{S}{N_C}; \Rightarrow r_c^2 = \frac{1}{\pi}\frac{S}{N_C} \tag{7}$$

$$d_{min} = \alpha \times \sqrt{\frac{S}{N_C}} \tag{8}$$

where S is area of sense field and s_c is area of each cluster that we assume in the best case, clusters have same area. r_c denotes radius of a circle with area equals to s_c. Also, α is a constant which must be set appropriately. The proposed LF clustering method consists of two phases: CHs selection and clusters formation.

The first phase's aim is selection of a set of nodes as CHs which its member have high level of stored energy and simultaneously the chosen set should be distributed as homogeneous as possible over the sense field. At any moment of the CHs selection phase, all nodes are classified in three sets: selected nodes as CHs (denoted by E). The Primary candidates, denoted by P, contains nodes that potentially can be chosen as a CH in term of homogeneity. The set of secondary candidates which have lower priority of being a CH; this set is denoted by S. At the beginning of process, it is obvious that all nodes can be chosen as CH and P includes all alive nodes of network and two other sets are empty. At the first step, a node with the most level of remained energy is selected as one of the intended CHs. The ID of this node is added to E and omitted from P. According to location of the recent selected CH, all of the close nodes lose their priority. The threshold distance for priority checking is d_{min}. Hence, after selection of each CH, any node which is located in a circular region with radius d_{min} around new elected CH leave out P and recognized as a secondary candidate. By checking the status of all nodes in P, the sets of secondary and primary candidates are updated. Then, next CH is selected from primary candidates in the same manner and afterwards, some nodes lose their priority. This procedure continues until selection of all required CHs or the primary candidates' set goes to empty. In the latter case, the remaining number of CHs are selected from secondary candidates. In order to maintain homogeneity of CHs' distribution, next steps are followed. First, distances to all current selected CHs in E are calculated for every secondary candidate in S. Among all distances of a node in S from members of E, the minimum one is considered as criterion which is denoted by d_E. After calculation of d_E for all of the secondary candidates, the node with maximum d_E is selected as new CH. The selected node leaves out S and becomes a member of E. The distance of all remained nodes in S to new CH are calculated. If the distance of any node to new CH is less than its d_E, the d_E value of the node changes to this distance. The next required selections continues similarly. For more clarification, the CHs selection phase is shown in Fig. 1 in summary.

In clusters formation phase, non-CH nodes make decision about pertaining to one of the CHs. At the first step of this phase, every CHs send an advertising message and nodes within their broadcast range receive this message. Non-CH nodes receive some advertising messages with different signal strength due to different distances between them and CHs in their broadcast range. Each non-CH node comprises the received advertising messages signals' strength as measure of connectivity to related CHs and selects the CH with most connectivity. After making decision, all non-CH nodes send an announcement message to declare their CH. CHs receive announcement messages and identify their cluster's members. They can devise an scheduling scheme like TDMA for their members to prevent collision in agreement process. Since this work mainly focuses on agreement and clustering scheme, it is presumed that each node can communicate with its intended node without interference however, links failures are considered.

B. Agreement

Agreement procedure consists of two levels. At the first level, agreement is implemented in each cluster and next, in the second level, CHs participate in an agreement process with agreed value of previous level. A BA algorithm called OPBA that tolerates links failure is used at the first and second levels which has been introduced by Yan *et. al* [16]. OPBA protocol reaches agreement by using the minimum number of rounds, even if the number of faulty components is $\lfloor \frac{n}{2} \rfloor - 1$, of which $\lfloor \frac{(n-1)}{3} \rfloor$ are faulty processors and the rest are faulty links. This algorithm is applied in each cluster at the first level. At the i^{th} cluster, number of faulty processors and links must satisfy the following two equations to reach successful agreement.

$$t_{p_i} \leq \lfloor \frac{(n_i - 1)}{3} \rfloor \tag{9a}$$

$$t_{l_i} < \lfloor \frac{n_i}{2} \rfloor - t_{p_i} \tag{9b}$$

where t_{p_i} and t_{l_i} denote the number of faulty processors and links in i^{th} cluster, respectively, and n_i denotes the number of i^{th} cluster's members. Each cluster with these two conditions reach a successful agreement. Since we considered malicious or faulty components do not cooperate, even if the number of defective components exceeds the allowable amount, nodes do not agree on a common wrong value and consequently agreement fails. Thus, almost all of CHs which their clusters can not reach correct agreement, participate in the second level with ϕ value that means agreement was failed in related clusters. However, it is possible to exist CHs with wrong data due to random coordinated faults.

At the second level, OPBA is applied on CHs. Because of CHs with ϕ and wrong values, there is a little possibility to fail agreement in overall. In such situations, the CHs can not agree on a common value, hence, we consider outcome value of biggest cluster which made successful agreement in the first level, as correct value. This value is more amenable, because biggest cluster characterizes state of network more than other ones. At the end of agreement phase, if CHs agree on a common value, the correct node with most energy level sends the agreed value to sink, otherwise, CH of biggest cluster sends its data.

IV. Simulations and Results

In this section, our proposed clustering and agreement methods are evaluated through simulations. We assume a typical WSN with following properties.

- All nodes are fixed.
- All nodes are equipped with transmission power control unit.
- Sensor nodes communicate in broadcast manner via an omnidirectional antenna.

Moreover, through Simulations, we consider communication medium and network structure's parameters according to Table I. For each experiment, we evaluate our scheme for 1000 different topologies at a certain number of nodes. First, the performance of clustering scheme is simulated. We compare our scheme with LEACH protocol and clustering method in [11] which is called EFC for brevity through this section. We consider X in (6) as a criterion for evaluation of different clustering methods. As seen in Fig. 2, our proposed method has the least average distance from optimal clustering and results in more homogeneous clusters selection that leads to communication cost reduction in next steps of network's operation. As network grows, the performance of EFC deteriorates, because it ignores some of selected CHs. In this simulation, we presume five percent of nodes are selected as CHs. It worth to note, X inevitably increases as network grows at any clustering method, because of a longer tuple of CD and larger components in CD_{opt}. However, behavior of average distance and its variation's gradient represent valuable information about efficiency of different methods in order to precise comparison. Moreover, based on experimental results, best performance of proposed method is achieved for $\alpha = 1 \sim 1.4$; hence, this parameter is set equal to 1.2 through simulations.

TABLE I
Simulation Parameters

Parameter	Value
The number of nodes	$40 \sim 140$
Field Size	$100m \times 100m$, $[0, 100]^2$
Free space (ε_{FS})	$10pJ/bit/m^2$
Multipath fading (ε_{MF})	$0.0013pJ/bit/m^4$
E_{elec}	$50nJ/bit$
CH percentage (p_{ch})	$5\%, 10\%, 15\%$
Initial Energy of sensor nodes	$2J \pm 1\%$

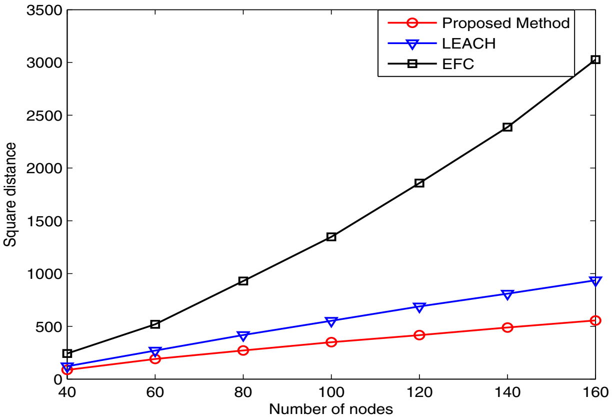

Fig. 2. Performance of proposed clustering method

Fig. 3 shows the communication overhead ratio of proposed method. Communication overhead ratio represents the number of exchanged messages in proposed method divided by exchanged messages in OPBA global agreement. Obviously, at any percentage of CHs and size of network, proposed method reduces communication overhead. Since in a global agreement, whole of network communicate with each other, communication overhead grows faster than proposed method. Hence, proposed method becomes more efficient for larger network in term of communication overhead ratio. The simulation is done for 1000 different topologies and 10 times for each topology

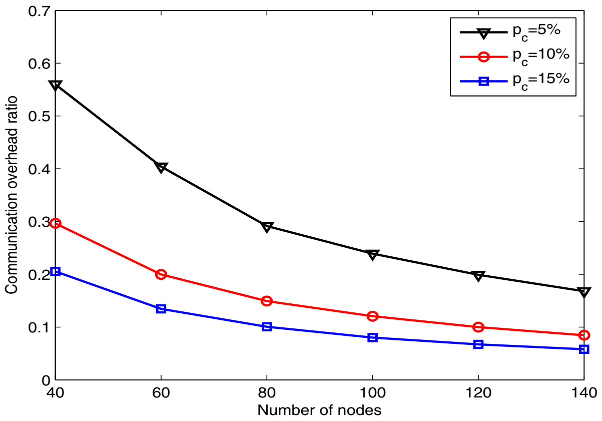

Fig. 3. Communication overhead of proposed method vs. OBPA

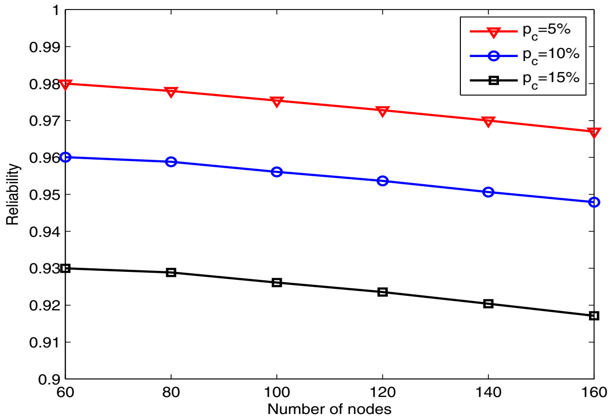

Fig. 4. Reliability of our proposed method.

and average communication overhead of OPBA and proposed method are calculated.

Fig. 4 represents the reliability of proposed scheme. For better evaluation, the number of faulty components set to maximum allowable value in OPBA global agreement, i.e. almost 33% of nodes are assumed as faulty nodes and number of faulty links in all clusters equals to 16% of network's size. The simulation results extracted from 500 different topologies and 20 different faulty components' distributions for each topology. Reliability is calculated as percentage of successful agreement among total attempts.

As we see, the reliability decreases with the number of nodes at a certain percentage of CHs, as well as, it reduces as CHs' percentage increases. Therefore, we can conclude that increasing number of CH at a network which results in further reduction of communication overhead, make network less reliable. There are a trade off between communication overhead and reliability so CH's percentage must be set accurately. Based on simulation, we can state that the best values for cluster percentage are $5 \sim 10$. In spite of a little reduction in reliability of system, the clustering and consequently reaching agreement in two levels are invaluable, owing to huge amount of energy conservation. Furthermore, we find that for a network with 20 nodes, if the unhealthy condition of network is given and four rounds are required, average energy consumption of nodes in OPBA is about $172\mu J$. However, if our proposed method is applied on same condition with 15% of CHs , i.e. three clusters, average consumed energy of nodes reduces to $283\mu j$. Unfortunately, the unhealthy condition of network is rarely known in advanced and the number of required rounds should be set according to maximum allowable number of faulty components. In such situation energy consumption of global agreement increases dramatically by size of network and implementation of global agreement methods, like OPBA, becomes impossible for large scale WSNs.

V. Conclusion

In this paper, we investigated applying the global BA in wireless sensor networks. We proposed a two level agreement based on a LF clustering approach. In our proposed method, first, nodes of each cluster agree on a common value and, then, CHs participate in final level of agreement. Clustering method tries to select CHs more homogeneously for equal size clusters formation which leads to reduction in number of message exchanges through agreement procedure. Therefore, our proposed method reduces communication overhead. Any increment in the number of clusters that is equivalent to increase the percentage of CHs, decreases the communication overhead, while it reduces reliability. By setting proper values for α which introduced in (8) and the percentage of CHs, our proposed method reaches agreement with reliability in favorable range. Owing to energy conservation and simultaneously acceptable reliability, implementation of our proposed method seems more practical than a global BA on whole network.

References

[1] L. Lamport and P.M. Smith, “Byzantine clock synchronization”, *ACM SIGOPS Operating Systems Review*, Vol. 20, no. 3, 1986, pp. 10-16.

[2] E.N. Hoch, D. Dolev and A. Daliot, “Self-stabilizing byzantine digital clock synchronization”, *Stabilization, Safety and Security of Distributed Systems, Springer Berlin Heidelberg*, 2006, pp. 350-362.

[3] F. Ye, H. Luo, S. Lu and L. Zhang, “Statistical en-route filtering of injected false data in sensor networks”, *IEEE Journal on Selected Areas in Communications, Special Issue on Self-organizing Distributed Collaborative Sensor Networks*, Vol. 23, no. 4, 2005, pp. 839-850.

[4] S. Zhu, S. Setia and S. Jajodia, “LEAP: efficient security mechanisms for large-scale distributed sensor networks”, *in Proceedings of the 10th ACM Conference on Computer and Communication Security*, 2003, pp. 62-72.

[5] L. Lamport, R. Shostak and M. Pease, “The Byzantine generals problem”, *ACM Transactions on Programming Languages and Systems*, Vol. 4, no. 3, 1982, pp. 382-401.

[6] D. Dolev, R. Reischuk and H.R. Strong, “Early stopping in Byzantine agreement”, *Journal of the ACM*, vol. 37, 1990, pp. 720-741.

[7] H.C. Hsieh, H. Ching, M.L. Chiang and M. Lun, “A new solution for the Byzantine agreement problem”, *Journal of Parallel Distributive Computation*, Vol. 71, no. 10, 2011, pp. 1261-1277.

[8] A. Achtzehn, Z. Benenson and C. Rohner, “Implementing agreement protocols in sensor networks”, *IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS)*, 2006, pp. 858-863.

[9] R. Klempous, J. Nikodem, R. radosz and N. Raus, “ Byzantine algorithms in wireless sensor networks”, *International Conference on Information and Automation (ICIA'06)*, 2006, pp. 319-324.

[10] K. Sun, "Secure distributed cluster formation in wireless sensor networks", *in Proceedings of the 22nd Annual Computer Security Applications Conference*, 2006, pp. 11-15.

[11] T. Kang, J. Yun, H. Lee, I. Lee, H. Kim, B. Lee and K. Han, "A clustering method for energy efficient routing in wireless sensor networks", *in Proceedings of the 6th World Scientific and Engineering Academy and Society (WSEAS) International Conference on Electronics, Hardware, Wireless and Optical Communications*, 2007, pp. 133-138.

[12] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks", *in Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, 2000.

[13] O. Younis and S. Fahmy, "Distributed clustering in ad-hoc sensor networks: A hybrid, energy-efficient approach", *in 23rd Annual Joint Conference of the IEEE Computer and Communications Societies*, Vol. 1, 2004.

[14] H. Ishii and H. Kakugawan, "A self-stabilizing algorithm for finding cliques in distributed systems", *in 21st IEEE Symposium on Reliable Distributed Systems*, 2002, pp. 390-395.

[15] T. Predrag and G. Agha, "Maximal clique based distributed group formation for autonomous agent coalitions", *in Coalitions and Teams Workshop (W10), 3rd International Joint Conference on Agents and Multi Agent Systems*, 2004.

[16] K.Q. Yan, Y.H. Chin and S.C. Wang, "Optimal agreement protocol in malicious faulty processors and faulty links", *IEEE Transaction on Knowledge and Data Engineering*, vol. 4, no. 3, 1992, pp. 266-280.