Secure Scheduling for Cluster-based TDMA Schedule MAC in Wireless Sensor Network

Dr. Pranav M. Pawar
Dept. of Computer Engg,
MIT-ADT, School of Engineering,
Rajbaug, Loni, Pune
pranav.pawar@mituniversity.edu.in

Prof. Nandkumar P. Kulkarni,
Dept. of IT, Smt. Kashibai Navale
College of Engineering, Pune
npkulkarni.pune@gmail.com

Dr. Dnyaneshwar S. Mantri,
Dept. of E & TC,
Sinhgad Institute of Technology,
Lonavala, Pune
dsmantri@gmail.com

***Abstract*— The overwhelming application growth of wireless sensor network (WSN) evolved the performance requirement of WSN in terms of security. The WSN is susceptible to many different security attacks but security attacks on medium access control (MAC) layer are more disastrous because the main role of MAC layer is to allocate and manage the available resources. The main aim of the paper is to explore the possibility of attack on cluster based MAC and to propose the solution to reduce or avoid the effect of attack in case of cluster-based time division multiple access (TDMA) schedule MAC. The paper give proposal of the cluster head (CH) attack on cluster-based MAC which attack on CH and increase the chances of CH re-election by draining the energy of CH and introduce the inter- and intra-cluster collisions. To diminish the effect of CH-attack paper put forward the idea of Secure-Green Conflict Free (S-GCF) which assigns the secure slots to CH and decreases the effect of CH-attack. The S-GCF shows better energy consumption, throughput and delay than cluster based TDMA schedule MAC Green Conflict Free (GCF) algorithm under CH-attack.**

Keywords- *WSN, security attack, MAC, TDMA, cluster, energy consumption, throughput, delay.*

I. INTRODUCTION

The WSN is expanding in a large way in terms of its application support and technology used to run those applications. This overwhelming growth of WSN increases the performance requirements of it by taking security into consideration. The security attacks on WSN reduce the performance by increasing energy consumption and delay with reduced throughput which are the major performance requirements of any WSN application [1, 2].

The security attacks effect on performance behavior of all layers of WSN protocol stack but it is vastly affected by the attacks happen on MAC layer. The WSN MAC security attacks are most hazardous because it straightly effects on allocation of available resources and they are difficult to detect [3]. The behavior and solution on security attack is varying according to type of MAC protocol and its level of hazards. It varies according to contention-, schedule-, and hybrid- MAC protocols [4, 5].

The paper concentrates on security attack happen on cluster-base MAC protocols where responsibilities are divided among CH to improve the energy efficiency and scalability of WSN. The key emphasis of paper is to inspect effect of security attacks on cluster-based MAC and to examine the solution on it.

The paper first proposes the CH-attack on cluster-based MAC mechanism. In case of this attack, intelligent attacker attacks on CH and starts its devastation. It effects on WSN in three ways, first by increasing chances of re-electing the CHs, second by introducing inter-cluster collision between malicious CHs aggregated packet with normal CHs aggregated packet and third by means of intra-cluster collision between normal node packet and reverse direction malicious packet coming from CH. The CH-attack on multiple CHs reduces the performance of GCF by 50%.

To reduce the destruction of CH-attack paper proposes secure scheduling algorithm S-GCF. The S-GCF algorithm considers two pools of slots, one is normal pool which consists of normal TDMA slots, and another one is secure pool which consists of secure TDMA slots. The algorithm assigns secure slots to all CHs and gateways by considering/assuming that they are transmitting or exchanging sensitive information (aggregated information). The secure slots assigns to the CHs prevents launching of CH-attack on CHs and helps to reduce destruction because of inducting the CH-attack.

To investigate the possibility of attack and its effect, paper uses a multi-hop cluster [6] based TDMA schedule MAC, GCF [7]. The GCF algorithm finds the single conflict free slot for each node across three hops. It shows reduced energy consumption, delay, and increased throughput with maximum reuse of slots and minimum conflict in the network. The comparative evaluation of GCF shows that GCF is the better algorithm in available state-of-the-art algorithms [7]. The S-GCF gives reduce energy consumption, delay, and good throughput than GCF under CH-attack.

The rest of this paper is ordered as follows: Section II describes the related work of WSN scheduling and its limitations. Section III defines considered system model and assumptions for cluster-based TDMA scheduling algorithm. Section III discusses the GCF algorithm with its flowchart; it also gives the proposal of CH-attack. The section IV explains the proposal of S-GCF which comprises secure slot assignment algorithm and features of secure slot. Section V discusses and presents the comparative results of GCF, GCF under CH-attack and S-GCF. Lastly, section VI concludes the work with future prospect.

II. RELATED WORK

In last few decades major work has been done in WSN scheduling. The WSN scheduling is classified according to the kind of approach or network used for scheduling algorithm. The different ways of classification are centralized- vs. distributed- scheduling, single- vs. multicolor- scheduling and flat- vs. cluster- network based scheduling. The section reviews some of the important development in it.

Grid-based Latin Squares Scheduling Access (GLASS) [8] is a flat network based distributed algorithm for assigning TDMA schedule. It tries to minimize the overhead cost to assign the schedule. Distributed Randomized Scheduling (DRAND) [9] algorithm reduces collision by using reliable data transmission but its overheads increases with scalability and mobility. Five-Phase Reservation Protocol (FPRP) [10] chooses the slot for each node by working in five phases and leads to increase in the overheads of the protocols. Deterministic Distributed (DD)-TDMA [11] gives good time

978-1-5386-5201-5/18/$31.00 ©2018 IEEE

and message complexity by deciding slot as per the neighbor information. The Distributed Neighborhood Information Based (DNIB) [12] algorithm also chooses its slots by collecting information from nodes neighborhood with retrieval process. The Power Efficient and Delay Aware Medium Access Control for Sensor network (PEDAMACS) [13] is a polynomial time distributed slot assignment mechanism. It shows reduced delays proportional to the number of nodes in a network [13]. Some algorithm like distributed link based scheduling algorithm [14] diminishes the communication latency in multi-hop wireless networks. The limitation of algorithm is to have constant topology.

The adaptive slot distribution algorithm is based on feedback mechanism [15]. It depends on collision feedback by the local nodes. It shows reduced interference under light load situation and also shows better efficiency in case of overlapping of clusters. The algorithm gives good scalability in case of inter-cluster communication and does not take-care density variations inside the cluster. The variable slot assignment algorithm [16] removes slot idle time while nodes continue to be active with no data to transmit or receive. Code Division Multiple Access (CDMA) codes are used for evading the interference, which increases its complexity. In Adaptive DRAND (A-DRAND) [17], maximum slots are assigned to CH. The slots assigned to CHs are get alternated for balancing an energy by other cluster members, which leads to increased overheads. The group based scheduling algorithm [18] reduces energy consumption, at every iteration, of slot assignment. It is not flexible to varying traffic situations. The GCF is single color algorithm for cluster-based network, which assigns conflict free slot across three hops. This algorithm shows better performance than existing scheduling algorithm [7]. The extension of this algorithm is Multicolor-GCF (M-GCF), it allocates set of conflict free slots across three hop view [19]. The GCF and M-GCF shows good energy efficiency with scalability and they also help to adapt the changes, if node changes its position.

The major limitation of scheduling algorithm for flat network is that they do not gives good scalability for denser scenarios of WSN and shows reduced efficiency of slot sharing. This problem of flat network based scheduling is solved by cluster based scheduling algorithms which are energy efficient with good scalability. All these scheduling algorithms are developed without taking security into consideration i.e. by checking the possibility of attack on the scheduling algorithms and defense mechanism against the attack. The main motivation of the paper is to understand the possibility of attack under cluster based scheduling algorithm and to find the solution to reduce the effect of attack.

III. System Model and Assumptions

A. Assumptions

1) Node Assumptions: Every node has identical characteristics. Every node is not aware of location. Each node considers distinctive ID and assumed to be synchronized with all. Every node acquire slot from two pool of slots, one is normal pool of slots for normal node and another one is secure pool which consist of secure slots for CH who are aggregating and transmitting aggregated information. Node requires single slot for performing multi-hop communication.

2) Network Assumptions: The network considers one base station (BS) or sink node. It is partitioned in clusters; every cluster has normal nodes and a CH. Here, for achieving an energy efficiency and scalability of network, the clusters are assumed to be multi-hop. The BS, CH and normal nodes are considered to be static nodes. The links in a network are assumed to be bidirectional.

B. System Model

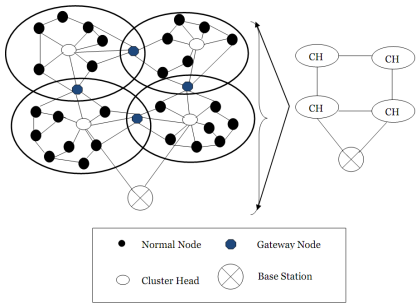

Figure 1. System model [7]

Figure 1 shows the system model for proposed algorithm. The network is considered as graph G (V, E). *V* is the set of vertices/nodes and E is the set of edges/links. The graph *G (V, E)* is partitioned into cliques (clusters), *G= {G1, G2, …….. Gn}*. The research considers multi-hop clustering algorithm for forming clusters. The CH is acting like a BS for each cluster, which gathers data from all cluster members. The gateway nodes are common nodes between clusters, which helps to connect clusters together. [7].

Here, each node needs a slot to do communication. In this model the CH and gateway nodes will get the slots from secure pool which consists of secure slots and normal nodes will get the normal slots from normal slot pool. Here, considered that the secure pools have less number of slots than normal slot pool.

IV. CH-Attack on Cluster-Based MAC Algorithms

Figure 2 shows the activity modeling of the proposed security attack on cluster-based MAC algorithms. The CH-attack considers that the intelligent attackers have full knowledge about sensor network and cluster-based MAC protocol used. Here, the attacker is said to be an intelligent attacker because he can differentiate between normal node and CH node and they will initiate an attack only if node is CH.

The reason behind to attack on CH is that, CH is liable for gathering data from cluster members (intra-cluster communication) and transmitting the accumulated data to other CH or to the BS (inter-cluster communication). Therefore, attack on CHs harm more than attacks on normal node. The CH-attack leads to increase energy consumption because of inter- and intra- cluster collision deplete the energy of nodes earlier and leads to earlier partition of total network and cluster.

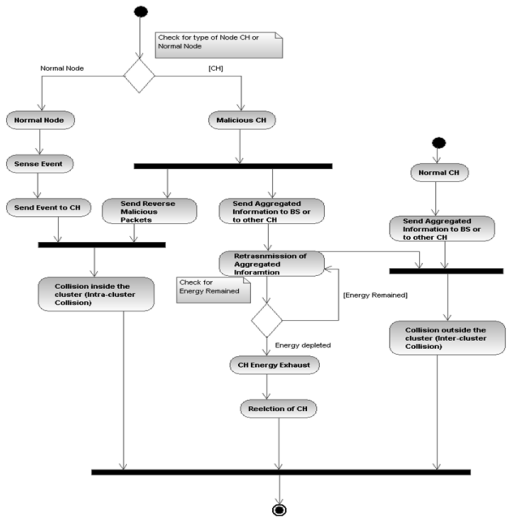

Figure 2. Activities under CH attack

V. S-GCF: SECURE-GCF ALGORITHM

The previous section explained the CH attack on cluster-based MAC mechanism, which reduces efficiency of a network (energy consumption, throughput, and delay). Hence, it is required to avoid or save the network from CH-attack. This section explains a new proposal S-GCF for assigning the slots to the nodes, for avoiding the effect of CH-attack. The S-GCF algorithm suggested here assigns the normal slots to normal nodes from normal slot pool while it assigns secure slots to CH and gateway nodes from secure slot pool by considering that CH and gateway nodes are transmitting/communicating sensitive information in a network. The S-GCF algorithm helps to save the WSN from CH-attack by allocating secure slots to CH and gateway nodes.

A. Notations

- $GC = (V_c, EC)$ is the conflict graph of G with V_c nodes/vertices and EC links/edges.
- d is the degree of node.
- N_{1v} , N_{2v}, N_{3v} are a list of one hop-, two hop-, and three hop- neighbors of node v respectively.
- v is the n ode whose slot is already known.
- I is the set of normal slots, $I = \{0,1,2,3,\ldots\ldots,i\text{-}1\}$
- S is the set of secure slots, $S = \{0,1,2,3,\ldots,s\text{-}1\}$ where $size\ of\ S < size\ of\ set\ I$ i.e. number of secure slots are less than normal slots.
- $D[n]$ is the set of degree of each node in GC.
- N is the set of all nodes in a network. n is the number of nodes in set N.
- BN is the set of all boundary nodes (gateway) in a network, $BN \in N$, bn is the number of boundary nodes in BN, $bn < n$.
- CHN is the set of all cluster head nodes in a network, $CHN \in N$, chn is the number of CH nodes in CHN, $chn < n$.

B. Secure Slot Assignment Algorithm

The algorithm for secure slot assignment takes conflict graph GC as input and gives output as assignment of normal slots to normal nodes and secure slots to CH or gateway nodes. The algorithm first calculate the degree of nodes, one-, two- and three- hop neighbors of each node and sort the list of nodes using degree of nodes. In the next part, algorithm check for each node, if node u belongs to N then it assign normal slot to node u otherwise, if node u belongs to BN or CHN then assign the secure slot to node u. The algorithm for secure slot assignment is as follows,

Input: *Conflict graph $GC= (V_c, EC)$ of each sub graph $G= \{G_1, G2,\ldots\ldots,G_n\}$*

Output*: The nodes with normal slot or secure slot according to requirement.*

```
Begin
for each node v ϵ Vc do
        Calculate degree d.
        D[n] = d
        Calculate N1v, N2v and N3v.
end for
sort (D[n])
for each node u ϵ D[n] do
        if ((u ∈ N) && (u ∉BN) && (u ∉CHN)) then
                Assign slot i from normal slot pool I
                n=n+1
                i=i+1
        else if ((u ∈ N) && (u ∈ BN) && (u ∉CHN)) then
                Assign secure slot s from secure slot pool S.
                n=n+1
                bn=bn+1
                s=s+1
        else if ((u ∈ N) && (u ∉BN) && (u ∈CHN)) then
                Assign secure slot s from secure slot pool S.
                n=n+1
                chn=chn+1
                s=s+1
        end if
        end if
        end if
end for
end
```

C. Features of node with Secure Slot

The algorithm explained in previous section assigns the secure slot to the CH and gateway nodes. These are the nodes that are transmitting the aggregated information which influence the most of the nodes in a network. For example, CH is aggregating all information from all the nodes in a cluster and forwarding towards other CH or BS via some gateway nodes. Another considered sensitive transmission is transmission between CH and gateway nodes. Therefore, the transmission mechanism used by the nodes that have secure slot is different from nodes that have normal slot. Whenever the nodes with secure slot want to transmit the information to other nodes it will check the following conditions,

- The node is CH or gateway node or not.
- The node having secure slot or not.

Before transmission, the source node with secure slot will confirm the above two conditions then it will transmit the authentication message towards destination node. If destination node is the correct destination then it will send

authorization message and then they will start to transmit actual data packets. The pair wise authentication scheme [20] is used for the exchanging the authentication and authorization information. Here, each CH or nodes with secure slots marinating its own key and before starting the communication they are exchanging the key among themselves.

D. Transmission algorithm of nodes with secure slot

The algorithms explain the transmission of nodes with secure slot. The input of the algorithm is source node *u* with secure slot *s* and destination node *v*. The algorithm first checks that the destination node *v* has secure slot or not, if *v* has secure slot then *u* transmit the authentication message to node *v* and if node *v* is the correct destination then *v* transmit the authorization message to node *u*, once the node *u* will receive authorization from node *v* then it will start transmission with node *v*. The algorithm is as follows,

Input: *Source node u with secure slot s and destination node v.*

Output: *Confirmation of destination node v with secure slot and confirmation for transmission in between u and v*

Begin
if *(v ϵ N) && (v ϵ BN) && (v ϵ CHN)* ***then***
    v have secure slot s
end if
if *v have secure slot s* ***then***
    u transmit authentication message to node v
    if *(node v will receive authentication message) && (node v is the correct destination) then*
        v transmit authorization message to node u
    end if
end if
end

VI. SIMULATION AND RESULTS DISCUSSION

A. Simulation Details

The Network Simulator-2 (NS-2) is used for the simulation of the GCF, GCF under CH-attack and S-GCF. The nodes are organized uniform randomly in a given area. The Enhanced Multihop Clustering Algorithm (EMCA) [21] is used for cluster formation. Table I shows the simulation parameters considered for simulation. The implementation of S-GCF algorithm uses simple pair wise authentication mechanism.

B. Results and discussions

Figure 3 shows the comparative average energy consumption of GCF, GCF with CH attack and S-GCF. The trend shows that average energy consumption of GCF is increased in large amount in presence of CH attack. CH attack can make the differentiation between normal node and CH, it attacks on to the CH and make it malicious CH. These malicious CHs in a network are retransmitting the already transmitted aggregated information and transmit the reverse malicious packets towards the normal node inside the cluster. This extra traffic in the network requires the extra energy to generate and transmit it, which leads to increase in energy consumption. The effect of CH attack is reduced in large extent in case of S-GCF but it is not equal to the energy consumption of GCF. The reason for is the kind of secure slot assignment technique used to assign the slot to CHs. In this case, if attacker will try to attack on CH it will not be authenticated by CH because of its secure slot and it will prevent the attack and its effect, but some energy is required for generating and transmitting the authorization and authentication message. The extra authentication and authorization messages lead to additional energy consumption in case of S-GCF than GCF.

TABLE I. SIMULATION PARAMETER

Parameter Name	Setting Used
Network Interface Type	Wireless Physical
Radio Propagation Model	Two-Ray Ground
Antenna Type	Omni-directional Antenna
Channel Type	Wireless Channel
Interface Queue	Priority Queue
Buffer size of IFq	50
MAC	GCF, S-GCF
Routing Protocol	Ad-hoc Routing
Initial Energy (Joule)	100
Idle Power (mW)	14.4
Receiving Power (mW)	14.4
Transmission Power (mW)	36.0
Number of Nodes	25, 50, 75, 100
Number of sources	24, 49, 74, 99
Number of BS	1
Placement of nodes and BS	Uniform random placement for nodes and BS is located at center of the network.
Amount of malicious nodes	50%
Number of simulation runs	50

Figure 4 illustrates the average delay of GCF, GCF with CH attack and S-GCF. The results of this three cases shows that average delay of GCF in presence of CH attack is increased. The reasons of increased delay are, first malicious CHs in a network regenerate the aggregated information and transmit it towards other CH or BS and second it also transmits some malicious packets towards the normal node. The regenerated aggregated packets and normal malicious packets from CH introduce the additional delay by two ways, time require for transmitting them and they also leads to some collision in inter-cluster and intra-cluster collision. This collision in network incurs bonus delay and energy consumption. The amount of delay is reduced in case of S-GCF but increased than GCF because of authorization and authentication messages it uses, which reduce the effect of attack but some time it introduce extra delay because of extra messages transmission.

The comparative graph shown in figure 5 explains the trend in average throughput of GCF, GCF with CH attack and S-GCF. It shows that the performance of GCF reduces because of CH attack but minimized by using S-GCF. The graph shows approximately the same throughput of S-GCF with GCF because of secure slot it uses for CH transmission which prevents the CH attack on CHs.

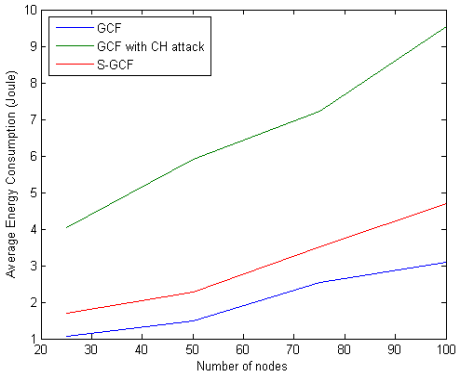

Figure 3. Measurment of average energy consumption

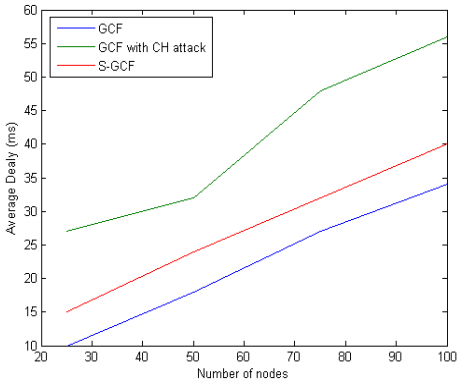

Figure 4. Measurement of average delay

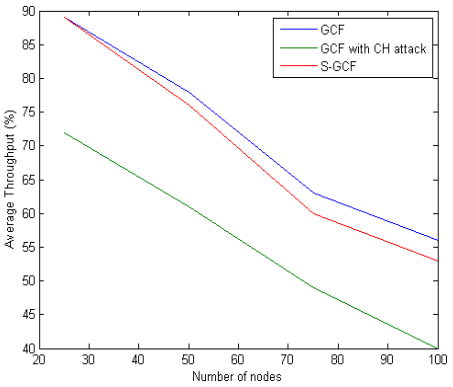

Figure 5. Measurement of average throughput

VII. Conclusion and Future Work

The paper gives the proposal of attack on cluster-based MAC i.e. CH-attack, which reduces the overall performance and behavior of WSN in terms of energy consumption, throughput and delay by increasing the chances of running the CH election algorithm for re-electing the CH and by introducing inter- and intra- collision in large amount. The paper suggests the solution to avoid or reduce the effect of CH-attack by introducing new schedule assignment algorithm S-GCF. S-GCF reduces the effect of attack by assigning secure slots to CH, which is transmitting sensitive information (aggregated information). The algorithm shows improved energy consumption, throughput and delay than cluster-based TDMA schedule MAC GCF under CH attack.

In future, the work can be extended by measuring the performance of S-GCF by considering different kind of authentication and authorization mechanisms. This performance results will be useful to develop specific kind of authentication mechanism for secure MAC. The work can also be extend, to explore more possibilities of attack in cluster-based MAC mechanism and to find a solution on it.

References

[1] Giuseppe Anastasi, Marco Conti, Mario Di Francesco, Andrea Passarella., "Energy Conservation in Wireless Sensor Networks: A survey.", Elsevier Ad hoc Networks. Vol. 7, Issue 3, 2009, 537–568

[2] Gianfranco Cerullo, Giovanni Mazzeo, Gaetano Papale, Bruno Ragucci, Luigi Sgaglione, "Chapter 4 - IoT and Sensor Networks Security", Security and Resilience in Intelligent Data-Centric Systems and Communication Networks, Academic Press, 2018, 77-101.

[3] Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Shingo Ohmori, & Ramjee Prasad, "Behavioral Modeling of WSN MAC Layer Security Attacks: A Sequential UML Approach", Journal of Cyber Security and Mobility, River Publishers, Vol.1. Issue 1, 2012, 65–82

[4] Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Shingo Ohmori, & Ramjee Prasad, "Hybrid Mechanisms: Towards an Efficient Wireless Sensor Network Medium Access Control", WPMC, Brest, France, 2011, 492-496.

[5] Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, & Ramjee Prasad,, "GHMAC: Green and Hybrid Medium Access Control for Wireless Sensor Networks", Springer Wireless Personal Communications, Volume 94, Issue 3, 2017, 1839–1868.

[6] Ammeer Ahmed Abbasi, Mohamed Younis, "A Survey on Clustering Algorithms for Wireless Sensor Network", Elsevier's Computer Communication, Vol. 30, 2007, 2826-2841.

[7] Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Shingo Ohmori, & Ramjee Prasad, "GCF: Green Conflict Free Scheduling Algorithm for WSN", IEEE ICC-E2Nets Workshop, Ottawa, Canada, 2012, 5795-5799.

[8] Chih-Kuang Lin, V. Zadorozhny, P. Krishnamurthy, Ho-Hyun Park, and Chan-Gun Lee, "A Distributed and Scalable Time Slot Allocation Protocol for Wireless Sensor Networks", IEEE Transactions on Mobile Computing, , Vol. 10, Issue 4, 2011, 505–518.

[9] Injong Rhee, A. Warrier, Jeongki Min, and Lisong Xu. Drand, "Distributed randomized TDMA Scheduling for Wireless Adhoc Networks", IEEE Transactions on Mobile Computing, Vol. 8, Issue 10, 2009, 1384–1396.

[10] Chenxi Zhu and M.S. Corson, "A Five-Phase Reservation Protocol (FPRP) for Mobile Adhoc Networks", INFOCOM '98, San Francisco, CA, USA, Vol. 1, 1998, 322–331.

[11] Yu Wang and I. Henning, "A Deterministic Distributed TDMA Scheduling Algorithm for Wireless Sensor Networks", WiCom, Shanghai, China, 2007, 2759–2762.

[12] Ines Slama, Bharat Shrestha, Badii Jouaber, Djamal Zeghlache, Tapio J. Erke, "DNIB: Distributed Neighborhood Information Based TDMA Scheduling for Wireless Sensor Networks", VTC, Calgary, BC, Canada, 2008, 1-5.

[13] S.C. Ergen, P. Varaiya, "PEDAMACS: Power Efficient and Delay Aware Medium Access Protocol for Sensor Networks", IEEE Transactions on Mobile Computing, Vol. 5, Issue 7, 2006, 920–930.

[14] Shashidhar Gandham, Milind Dawande, Ravi Prakash, "Link Scheduling in Wireless Sensor Networks: Distributed Edge-coloring Revisited", Journal of Parallel and Distributed Computing, Vol. 68, Issue 8, 2008, 1122 – 1134.

[15] Wu T., Biswas S., "A Self Reorganizing Slot Allocation Protocol for Multi-cluster Sensor Network", IPSN, UCLA, Los Angeles, California, USA, 2005, 309-316.

[16] Hussain, S., Zahmati, A. S., Fernando, X., "LASA: Low-energy Adaptive Slot Allocation Scheduling Algorithm for Wireless Sensor Networks", SARNOFF, Nassau Inn, Princeton, NJ, USA, 2009, 1-6.

[17] Shihan Li, Depei Qian, Yi Liu, Jie Tong, "Adaptive Distributed Randomized TDMA Scheduling for Clustered Wireless Sensor Networks", WiCOM, Shanghai, China, 2007, 2688-2691.

[18] Tao Shu, Marwan Krunz, "Energy-efficient Power/Rate Control and Scheduling in Hybrid TDMA/CDMA Wireless Sensor Networks", Computer Networks: The International Journal of Computer and Telecommunications Networking, Vol. 53, Issue 9, 2009, 1395–1408.

[19] Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Shingo Ohmori, Ramjee Prasad, "M-GCF: Multicolor Green Conflict Free Scheduling Algorithm for WSN", IEEE WPMC, Taipei, Taiwan, 2012, 140-144.

[20] Yang Xiao, Venkata Krishna Rayi, Bo Sun, Xiaojiang Du, Fei Hu, Michael Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks", Elsevier Computer Communication, Vol. 30, 2007, 2314-2341.

[21] Ying Qian, Jinfang Zhou, Liping Qian, Kangsheng Chen,"Highly Scalable Multihop Clustering Algorithm for Wireless Sensor Networks", ICCCAS.2006, Guilin, Guangzi, China, 1527-1531.