ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

PAD: Power Aware Key Distribution in Wireless Sensor Network Using Group Configuration Methodology

M. Raghini[1], Dr. N. Uma Maheswari[2], Dr. R. Venkatesh[3]

[1]Department of Computer Science & Engineering, K L N College of Engineering, Sivanagangai, Tamilnadu, India

[2]Department of Computer Science & Engineering, PSNA College of Engineering, Dindigul, Tamilnadu, India

[3]Department of Information Technology, PSNA College of Engineering, Dindigul, Tamilnadu, India

Abstract— Distributed Wireless Sensor Network (DWSN) is an emerging technology for information gathering and processing. A sensor network consists of much resource constrained sensor nodes. These nodes perform measurements of some physical phenomena, process data, gather reports and send these reports to the central processing unit called Mobile Sink (MS). Such communication must be secure in military surveillance, intelligence and tracking field. Efficient key management technique is essential to provide secure communication. As sensor nodes are battery powered devices, the critical aspects in facing key distribution are how to reduce the energy conception for the components of sensor nodes. Thus, implementing a key distribution algorithm should possess a minimum power conception. The proposed work steps towards greater heights by integrating power module with pairwise key establishment using group configuration methodology. Further, we present an investigation of power consumption using STEM (Sparse Topology and Energy Management) protocol on sensor nodes (SNs) during the pairwise key establishment using graphical tools. Analytical results of this PAD (Power Aware Key Distribution) show that energy efficiency is increased with sensor nodes while establishing pairwise key using group configuration when compared to existing key pre-distribution techniques.

Keywords— Distributed Wireless Sensor Network (DWSN), Mobile Sink (MS), Pairwise Key Establishment, Power Consumption, Sparse Topology and Energy Management (STEM), Power Aware Key Distribution (PAD).

DWSN contains a number of SNs that are deployed over a geographical area to sense the desired phenomena. Typically, a sensor node includes the basic components such as sensing subsystem, processing subsystem and a power unit [1]. The power of DWSN lies in the ability to deploy large number of tiny nodes that assemble and configure themselves. Usage scenarios for those devices range from real time tracking, monitoring environmental conditions, defense, security and monitoring health related equipment. The entire application arena, which assigns a major role to sensor nodes in order to sense information, must be highly secure. This security is one of the major issues when sensor nodes are deployed in a hostile environment. Every SN senses the data, collaborate it and send it to MS [14] [15]. Such information traversal can be securely governed by key distribution algorithm. In point of maintaining secure communication using key distribution, compromising the energy of sensor node is no way advisable. Thus a low power key distribution is essential for DWSN. On the other hand the security of WSN is no way compromised in terms of adversary attack, compromised node replication attack [8] [10] [12]. During Key distribution, generating a key from the processing unit consumes less energy, but the pairwise key establishment between two SNs which is performed prior to data transmission consumes more energy. Many energy conservation schemes are available which performs an eminent role in minimizing the energy during transmission. Those schemes are discussed in Table.1.

TABLE I
POWER SAVING SCHEMES FOR WIRELESS SENSOR NETWORK

Duty Cycling	Topology Control	Location Driven	
		Connection Driven	
	Power Management	Sleep/Wakeup	On-Demand
			Scheduled Rendezvous
			Asynchronous
		MAC Protocols with Low Duty Cycle	TDMA
			Contention Based
			Hybrid
Data Driven	Data Reduction	In-Network Processing	
		Data Compression	
		Data Prediction	
	Energy Efficient Data Acquisition	Adaptive Sampling	
		Hierarchical Sampling	
		Model-Driven Active Sampling	
Mobility Based	Mobile Sink		
	Mobile Relay		

Table.1. Give a detailed view on power saving modes for WSN [17]. It is broadly classified into Duty Cycling [19], Data Driven and Mobility Based. In this work we implement a pairwise key pre-distribution scheme using group configuration and also analyzed how it works when a power consuming protocol is running on the top of MAC protocol. This way of combining the concept of key pre-distribution and power conception leads to PAD which significantly changes the performance of SNs in terms of their power utilization.

II. RELATED PAIRWISE KEY PRE-DISTRIBUTION SCHEMES

A. Random Pairwise Key Pre-Distribution

It is a basic approach for key pre-distribution, where a distinct number of cryptographic keys that can be stored on a SN. The functions are defined in three phases called, initialization phase, middle phase and final phase. Before sensor nodes are deployed, an initialization phase is performed. The basic approach picks a random pool of keys 'P' out of the total possible key space 'KP'. Key Rings are randomly selected from the key pool 'P' and stored in the sensor node's memory, where 'R' is the key ring. The number of keys in the key pool |P|, is chosen such that the two random subset of size |R| in P will share at least one common key with some probability 'p' [2] [3] [4] [5] [6].

The SN discovers the common key, to perform out, with which of their neighbors they want to share the key. The initialization phase is completed by forming a secure link using the common keys. After key deployment, the middle phase sets up a path keys with nodes out of their vicinity. The path can be found from a source SN to its neighbor using graph connectivity. Forwarding to the final phase, transmission power is efficiently increased due to unremitting performance of multihop range extension communication with all the base station.

B. Q-Composite Pairwise Key Pre-Distribution

Q-Composite is a process of finding q number of common keys among the neighbors, instead of just one. By increasing the number of keys, automatically the resilience of the network also increases against node capture. As the resistance against the node replication and node degree is not constrained and there is no limit on the number of times each key can be used [2] [3] [4] [5] [6] [9] [11] [13] [16]. The number of keys on the key ring of any two SNs is considered as m which is picked from the key pool 'S'. Let the possible ways to select m from 'S' is A .The number of ways to select q common keys is 'B', then the remaining keys in the key ring of any two SNs are $2(m\text{-}q)$ and this can be achieved by 'C' number of ways. $2\ (m\text{-}q)$ is partitioned between the two SNs. Thus the probability of choosing q common keys in both the key rings is given by,

$$P\ (q) = (B)\ (C)\ (D) / (A) \qquad [1]$$

Hence $p\ (q)$ is the probability of identifying q common keys from the key rings to establish the pairwise key. Q-composite scheme is more secure against small-scale node capture as compared to basic scheme, but the deficiency is not scalable.

C. Probabilistic Pairwise Key Pre-Distribution

Probabilistic generation key pre-distribution scheme based on random key pre-distribution methodology. The scheme carried out by considering a key pool S whose size is measured by $|S|$, this key pool is available with a small number of generation keys K_r. Allocation of Keys to SNs is categorized based on power levels of SNs. By applying the hash algorithm to each generation key and publicly known seed value which is assumed as a password, a key chain $[K_{CHAIN}]$ is generated [2] [3] [4] [5] [6]. Every K_{CHAIN} has unique identifier ID_x [20]. Each low power SNs are loaded with random generation keys K_r. From K_r, $K_r * N$ random keys are calculated where $N = |S| / K_{CHAIN}$. Each high power SNs are loaded with random generation keys K_m picked from K_{CHAIN}, we're always $K_m > K_r$. Hence the probability of communication between two host is certainly occurring by choosing the common key either from generation keys K_r of low power SNs or from K_m of high power SNs [7] [9] [11] [13]. For large networks, a probabilistic method is more efficient than a deterministic method. This mechanism gives the effective result that all the nodes in the entire networks are almost fully connected with the probability of 0.9997. The probability of each node which can establish a pairwise key with its neighbor nodes is 0.33.

D. Polynomial Pool Based Key Pre-Distribution

Polynomial pool key pre-distribution schemes randomly generate bivariate t-degree polynomials with coefficients using key setup server, GF (λ), where λ is a prime number large enough to hold a cryptographic key. The polynomials have the property of f (x, y) = f (y, x). A unique identification is assigned to each polynomial share in the setup server to recognize the different polynomial.

Distributing polynomial share to individual nodes encourage direct key establishment between any two SNs when a common key is available [2] [3] [4] [5]. On the other hand, unavailability of common key leads to path key establishment where the commonality is recognized

by a neighboring node which acts as an intermediate node between these two nodes [6] [9] [11] [13].

The pairwise key pre-distribution schemes that were discussed above in the sections 2.1, 2.2 and 2.3 have proved that the pairwise key establishment within SNs have reduced the compromising of SNs but the power utilization and energy efficiency factor is not analyzed efficiently. Any power consuming protocol that is suitable for different schemes can measure the performance of SNs in terms of power utilization. Thus the forth coming PAD focuses on power utilization of SNs when generating and distributing keys with use of an efficient duty cycling protocol.

III. PAD METHODOLOGY

A. Random Key Generation

The proposed work starts by generating the keys using random function. The keys are generated according to the input needed for group configuration. The size of the key is dependent on the type of SN used. For example, test bed implementation can carry out using MICA SNs which is configured by ATmega 103 microcontroller, TR1000 radio 50kbit/s, with nesC programming and TINYOS Support. Also WASPMOTE sensor which is having enough battery backup can also be used.

Algorithm for random key generation

```
genRandom(randomrange)
    1.  RETURN Random().nextint(randomrange)
genRandom(randomrange,displaycount)
    2   For(i=0;i<displaycount;i++)
    3.  keys[i]=genRandom(randomrange)
    4.  END FOR MAIN(String [] args)
    5.  randomrange=6
    6.  displaycount=1
    7.  RANDOMNUMBER.genRandom
        (randomrange,displaycount)
```

B. Group Configuration for Pairwise Key Establishment

Group configuration is initiated by using a combination method which is very similar to the factorial distribution in the arrangement. Minimum number of keys are enough to generate pair of keys using combination method. For instance, if 'n' number of SNs is considered as one hop neighbors to mobile sink, only 'k' individual keys are enough to generate pair of keys for n nodes.

From number theory, the configuration of a non-negative integer 'k' denoted by k! is arranged. Its most basic occurrence is the fact that there is k! different ways to arrange k distinct objects in a sequence called permutation of *a* set of objects. Consider k! Where k>0, from the definition, the number of groups is identified using k-1. The first group is arranged using k! and all other groups are arranged as (k-x)!, where 1≤x<k-2

The factorial function normally defined by,

$$K! = \prod_{n-1}^{k} n \qquad [2]$$

Or recursively defined by,

$$K! = \begin{cases} 1 \\ (k-1)! \times k \end{cases}$$

$$if\ (k = 0)$$

$$if\ (k > 0) \qquad [3]$$

The number of groups can be identified and the arrangement of pair keys for *n* number of SNs can be determined. For instance, if *k*=6 i.e., 6 individual keys for *n* number of SNs. These 6 individual keys are generated from random function. The number of group *G*=*k*-1, so *G*=5. Assume the first group is G_1, this group can be arranged as *k*! i.e., 6! = 6x5x4x3x2x1. In this factorial arrangement pick x6 (first key) as common key for the group G1. Now the pair key for this group are (x6, x5), (x6, x4), (x6, x3), (x6, x2) & (x6, x1), this five pair of keys are assigned to five nodes of G1. G2 is arranged with (k-1)! i.e., (6-1)! = 5! = 5x4x3x2x1. Here the first key x5 is taken as a common key and the pair keys generated for 4 nodes of G2 is (x5, x4), (x5, x3), (x5, x2) & (x5, x1). Similarly G3 with (k-2)!, x4 as common key and the pair keys generated as (x4, x3), (x4, x2) & (x4, x1). G4 with (k-3)!, x3 as common key and the pair keys generated as (x3, x2) & (x3, x1). G5 with (k-4)!, x2 as common key and the pair key generated as (x2, x1).

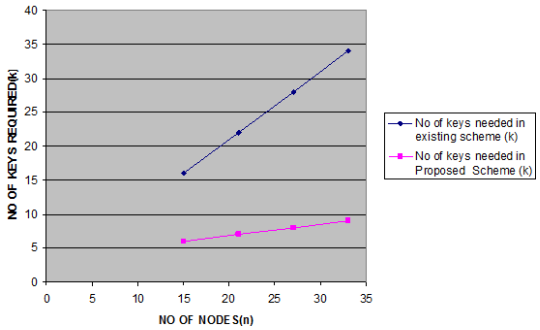

Fig.1. Comparison of key utilization in existing and proposed scheme

The node and key configuration of various groups is represented as follows, group *G1* where all nodes *n1*, *n2*, *n3*, *n4*, *n5* is having common key as *x6*. Whenever any two nodes want to establish the pairwise key, Let K_p denotes the initial key pool value that has been allocated for various groups under mobile sink. Let *x*, *y*, *z* is the chosen parameter C_p given by MS. The value of K_p , C_p and the common key of each group is given as input to the hash function g.

The above combination method of configuring the groups results in reduction in key utilization which is graphically shown in Figure.1.

If *n1* and *n2* wants to establish the pairwise key, then *x5* is computed to make a pair (*x6*, *x5*). Proving $g_{x6,\,x5} = g_{x5,\,x6}$ will enable the pairwise key establishment. i.e., a common key among two SNs will enable the pairwise key establishment between them. The same process is carried out for the remaining groups.

$$K_{x6,x5} = K_{x5,x6} = f(x6, x5) = [x + y\,(x6 + x5) + zx6x5]\ mod\ K_p \qquad [4]$$

C. STEM on MAC

The issue of power consumption is solved by duty cycling concept by implementing independent sleep/wakeup protocols running on the top of MAC protocol. Consumption of energy during pairwise key establishment is diminished due to sleep/wakeup procedure efficiency. Duty cycle is the major approach to reduce power consumption [17]. The most effective energy conserving operation is putting the radio transceiver in the low power sleep mode whenever communication is not required. In concern with our key pre-distribution, the transceiver is put in sleep mode when the MS is not distributing the keys and SNs is not establishing pairwise keys. The radio should be switched off as soon as there is no keys to distribute and pairwise key establishment is not needed. In this scenario, MS and SNs alternate between sleep and active periods depending on the network activity. This behavior is called as duty cycling. Duty cycle is defined as the fraction of time the SNs are active during their lifetime. As SNs performs a cooperative task, they need to coordinate their sleep/wakeup times. A sleep/wakeup scheduling algorithm thus accompanies any duty cycling scheme. It is typically a distributed algorithm based on which SN decides when to transit from an active state to sleep state and back. It allows neighboring nodes to be active which makes feasible way of key establishment even when nodes operating with low duty cycle. Integrating Sparse Topology and Energy Management (STEM) [18] [20] with pairwise key establishment is explained as follows.

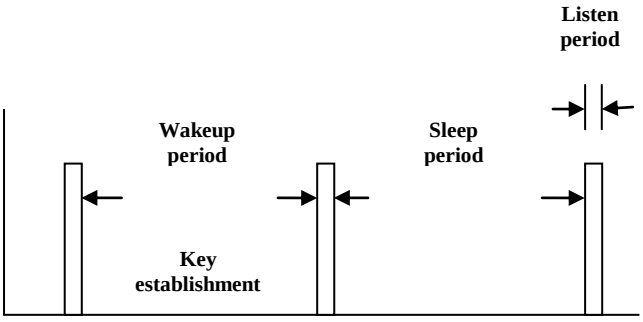

Fig.2. Duty cycle during key establishm

Figure.2. shows the assignation of key establishment during wakeup period. As per the novel suggested in PAD whenever any two SNs share a common key as formed from group configuration, they enable the pairwise key establishment successfully during the wakeup period. During listen period, every other node will be engaged in listening whether any of the SNs is waiting to transmit the sensed data so that the pairwise key can be established priory. And then the SN goes to sleep period i.e., the radio will be in off state.

STEM: STEM is a significant protocol to implement duty cycling concept. It uses two different radios for wakeup signal and key establishment. The wakeup radio is high power radio to increase the efficiency in terms of SNs ranges. Each SN turns on its wakeup radio for t_{energy} for t duration. When a source SN wants to establish pairwise key with the target SN, then it sends a stream of periodic beacons on the wake up channel. On receiving, the target SN sends the wakeup acknowledgement and turns on its own key establishment. If a collision occurs in the wake up channel, any SN that senses the collision activates its data radio "raised" for key establishment. Thus no acknowledgement is received during collision. STEM is executed on top of the MAC parallel during key generation, group configuration and pairwise key establishment. Since the least number of keys are utilized in our proposed work, this makes STEM in effective sense and results in very nominal power utilization in sensor nodes.

D. *Power Saving through Dry Run of STEM*

Power saved by running STEM is discussed in this section. Many research have shown that using twi frequency band for wakeup duration and for data transmission is efficient than using single band. As of now, we have used two bands correspondingly to calculate the total power consumed by a node n_1 during the time interval t. Initially it is represented as,

$$P_n = P_{active} + P_{key} \quad [5]$$

P_{active} is the power consumed during all the three periods i.e., wakeup, idle and listen respectively. Let P_{n1} represents idle power which combines P_{ir}, the idle and receive power. Let P_{tir} represents transmit, receive and idle power and t_{tir} is the transmit, idle and receive time.

$$P_{active} = P_{n1}\,(t - t_{tir}) + P_{tir}\,t_{tir} \quad [6]$$

$$P_{n1} = \frac{P_{sleep}(T - T_R) + P_{ir}\,T_R}{T} \quad [7]$$

By substituting [7] in [6] will emerge to calculate on part of the total power consumption. P_{key} is the power consumed during pairwise key establishment, t_{key} is the time during which the radio is ON. P_{kri} is the key reception and idle power during key establishment.

$$P_{key} = P_{sleep}\,(t - t_{key}) + P_{kri}\,t_{key} \quad [8]$$

Since idle periods are also fetched during key establishment, power of idle period during key establishment represented as P_{idle} is included in calculating the total power utilization. $P_{active1}$ represents the power utilization during key establishment in idle periods.

$$P_{active1} = P_{idle}\,(t - t_{key}) + P_{kri}\,t_{key} \quad [9]$$

From the equations [6] & [9],

$$\frac{P}{P_0} = \frac{P_{active}}{P_{active1}} \quad [10]$$

IV. RESULTS AND DISCUSSIONS

Power efficiency plays an important role in WSN. A typical method for designing a low power wireless sensor network is to reduce the duty cycle of each SN. Thus, our proposed work "PAD" investigates the level of power consumption while establishing pairwise key between SNs. It is shown graphically in Figure.3 that the power consumed by group configuration in PAD is less compared to existing schemes. This is due to the concrete

reason that less number of keys is enough to accommodate the number of nodes in group configuration and this is integrated with less power consumption by running STEM on top of the MAC.

E. Power Saving through Dry Run of STEM

Steps for running STEM on top of the MAC

STEP 1: Add New Agent

ns-allinone-2.34/ns.2.34/test folder/MyAgent.cc

STEP 2: Edit ns-allinone/ns.2.34/Makefile.in
Add the following line in OBJ_CC section
test/MyAgent.o \

STEP 3: Recompile NS-2
Open terminal and go to ns-allinone-2.34/ns-2.34 directory and type
./configure
make
make install

STEP 4: Run MyAgent.tcl file

STEP 5: Adding STEM protocol on MAC
ns-allinone-2.34/ns.2.34/test folder/MyStem.cc

STEP 6: Repeat STEP 2, 3 and 4 for MyStem.cc and corresponding MyStem.tcl file

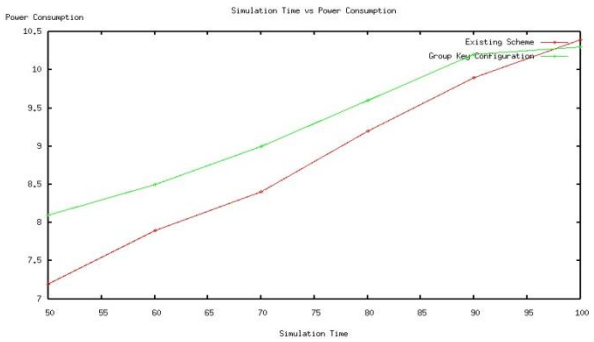

Fig.3. Graph Showing Comparison Chart of Power Consumption

V. CONCLUSION

The initial work was started with an attractive survey on various key pre-distribution methods using pairwise key establishment. Many works were successful, but the only common inconvenience found uniformly in all the results was the number of keys utilized for pairwise key establishment is increased. Obviously the power needed to generate such number of keys is increased. Also a separate power module was not concentrated in all the existing schemes. Thus the proposed work which is based on a factorial methodology for random group configuration reduces the number of keys generated. As a result the power consumption is decreased. A power module in the proposed work is implemented using STEM protocol integrates and employ duty cycling in SNs. This proves that the growth of outcome from group configuration methodology in significantly good when compared with existing schemes. The growth is shown by having a comparison of power between existing and proposed scheme, thus reaching noteworthy deeds

V. FOCUSING ON FUTURE PINNACLES

Currently we are working on sophisticated heuristics to generate optimized execution plans by concentrating on avoiding the maximum power utilization of an SN. The enhancement will be exhibiting common features by governing key generation process and authentication mechanisms. In the future, we plan to investigate the extension of our framework that how group configuration methodology can illustrate authentication among SNs while establishing keys. If such authentication is successfully done, then the power utilization can be measured again by running STEM on top of the MAC. This might result in securing the pairwise key establishment and highly flattened power utilization.

ACKNOWLEDGMENT

Greatest thanks go to Dr. N. Umamaheswari and Dr. R. Venkatesh for finding and actualizing the research topic. More details of this design are available in our technical report. We must also express our gratitude to anonymous, untraceable reviewers and committee members of the conference for their very helpful comments.

REFERENCES

[1] Akyildiz, F., W. Su, Y. Sankarasubramanian and E. Cayirci, 2002. A survey on sensor networks. IEEE Comm. Magazine,40:102-114.

[2] Amar Rasheed., Rabi N. Mahapatra, Key Predistribution Schemes for Establishing Pairwise Keys with a Mobile Sink in Sensor Networks. IEEE Transactions on Parallel and Distributed Systems, (TPTS ‘11), ACM, USA, pp: 174-184. DOI: 10.1109/TPDS.2010.57.

[3] Chan, H., A. Perrig and D. Song, 2003. Random Key Predistribution Schemes for Sensor Networks. In Proceedings of the 2003 IEEE Symposium on Security and Privacy, (SP ‘03), Washington, USA, ACM, pp: 197.

[4] Eschenauer, L. and V.D. Gligor, 2002. A key-management scheme for distributed sensor networks. In Proceeding of the ACM Conf. Computer communications Security (CCS’ 02), New York, NY, USA, pp: 41-47. DOI: 10.1145/586110.586117

[5] Liu, D., P. Ning and R. Li, 2003. Establishing Pairwise Keys in Distributed Sensor Networks. In Proceeding of the 10 th ACM Conf. Computers and Comm. Security (CCS ‘03), York, USAA CM, pp: 52-61. http://dl.acm.org/citation.cfm?id=948119

[6] M.Raghini., N.Uma Maheswari., R.Venkatesh, 2013. Overview on Key Distribution Primitives in Wireless Sensor Network. Journal of Computer Science, 9 (5): 543-550, 2013. ISSN 1549-3636.

[7] W. Stallings, “Cryptography and network security: principles and practice,” Prentice Hall, 1999.

[8] Adrian Perrig, John Stankovic, and David Wagner. Security in wireless sensor networks. *Commun. ACM*, 47(6):53–57, 2004.

[9] Martina Zitterbart and Erik-Oliver Blaß. An Efficient Key Establishment Scheme for Secure Aggregating Sensor Networks. In *ACM Symposium on Information, Computer and Communications Security*, pages 303–310, Taipei, Taiwan, March 2006. ISBN 1-59593- 272-0.

[10] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor Network Security: A Survey," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 1 1 , NO. 2, pp. 52-73,2009.

[11] W. Du,1. Deng, Y.S. Han, S. Chen, P.K. VarshneY,"A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge,”IEEE INFOCOM, 2004.

[12] J. Lopez and J. Zhou (Eds.), "Wireless Sensor Network Security", The Cryptology & Information Security Series (CISS), Vol. 1, lOS Press, 2008.
[13] W. Du, 1. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key predistributionscheme for wireless sensor networks," In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, October 27-31 2003, pp. 42-51.
[14] A. Rasheed and R. Mahapatra, " An Energy-Efficient Hybrid Data Collection Scheme in Wireless Sensor Networks," Proc. Third Int'l Conf. Intelligent Sensors, Sensor Networks and Information Processing, 2007.
[15] Y. Tirta, Z. Li, Y. Lu, and S. Bagchi, "Efficient Collection of Sensor Data in Remote Fields Using Mobile Collectors," Proc. 13th Int'l Conf. Computer Comm. and Networks (ICCCN '04), Oct. 2004.
[16] R. Rivest, "The MD5 Message-Digest Algorithm," RFC 1321, Apr. 1992.
[17] Giuseppe Anastasi, Macro Conti, Mario Di Francesco, Andrea Passarella, " Energy Conservation in Wireless Sensor Networks: A Survey," Ad Hoc Networks-Elsevier 7 (2009) 537-568.
[18] X. Yang. N. Vaidya, "A Wakeup Scheme for Sensor Network: Achieving Balance between Energy Saving And End-to end Delay", Proc of the IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS 2004), pp. 19-26, 2004.
[19] R. Zheng. J. Hou, L. sha," Asynchronous Wakeup for Ad Hoc Networks", Proc. ACM MobiHoc 2003, pp 35-45, Annapolis (USA), June 1-3, 2003.
[20] Schurgess.C, Tsiatsis. V, Srivastava. M. B, "STEM: Topology Management for Energy Efficient Sensor Networks", Proc of the IEEE Aerospace Conference, 3-1099-3-1108 Vol.3, 2002.