International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Certified and productive data communication for constellate wireless support system

[1] K.Syam & [2] R.Suresh
[1]M.Tech(CSE) , CREC, Tirupati, Email.Id: syamkami@mail.om
[2]Associate Professor, HOD, CSE, CREC, Tirupati, Email.Id: Ramsuri42@gmail.com

Abstract—
Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that, the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

Index Terms—Cluster-based WSNs; ID-based digital signature, ID-based online/offline digital signature; secure data transmission protocol.

I INTRODUCTION

MANETs feature self-organizing and independent infrastructures, which shows them an good choice for uses such as communication and information sharing. The openness and reorganization capabilities of MANETs. Nodes in MANETs are very easy to attacks mainly modifying and examine information and traffic analysis by communication eavesdropping or attacking routing protocols. Areas such as military applications (e.g., soldier communication) it's very critical. If a network created in a bottle field. Through traffic analysis, enemies may catch transmitted packets, trace our users(i.e., nodes),attack the main sender nodes, and distribute the data processing by acting as relay nodes, it leads more damage, so in MANETs to enhance secure communications with help of hiding node information and avoiding traffic analysis attacks from attackers. Anonymity in MANETs includes user information and area anonymity of data sources and destinations, as well as path anonymity."Identity and location anonymity of sources and destinations" means it is tough for other nodes to see the original identities and perfect are as of the sources and destinations. Secure data transmission is a critical issue for wireless sensor networks (WSNs).Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

II SYSTEM DESCRIPTION AND PROTOCOL OBJECTIVES

2.1 Network Architecture

Consider a CWSN consisting of a fixed base station (BS) and a large number of wireless sensor nodes, which are homogeneous in functionalities and capabilities. We assume that the BS is always reliable, i.e., the BS is a trusted authority (TA). Meanwhile, the sensor nodes may be compromised by attackers, and the data transmission may be interrupted from attacks on wireless channel. In a CWSN, sensor nodes are grouped into clusters, and each cluster has a cluster-head (CH) sensor node, which is elected autonomously. Leaf (non-CH) sensor nodes, join a cluster depending on the receiving signal strength and transmit the sensed data to the BS via CHs to save energy. The CHs perform data fusion, and transmit data to the BS directly with comparatively high energy. In addition, we assume that, all sensor nodes and the BS are time synchronized with symmetric radio channels, nodes are distributed randomly, and their energy is constrained.

2.2 Security Vulnerabilities and Protocol Objectives

The data transmission protocols for WSNs, including cluster based protocols (LEACH-like protocols), are vulnerable to a number of security attacks [2, 23]. Especially, attacks to CHs in CWSNs could result in serious damage to the network, because data transmission and data aggregation depend on the CHs fundamentally. If an attacker manages to compromise or pretend to be a CH, it can provoke attacks such as sinkhole and selective forwarding attacks, hence disrupting the network. On the other hand, an attacker may intend to inject bogus sensing data into the WSN, e.g., pretend as a leaf node sending bogus information towards the CHs. Nevertheless, LEACHlike protocols are more robust against insider attacks than other types of protocols in WSNs [23]. It is because CHs are rotating from nodes to nodes in the network by rounds, which makes it harder for intruders to identify the routing elements as the intermediary nodes and attack them. The characteristics of LEACH-like protocols reduce the risks of being attacked on intermediary nodes, and make it harder for an adversary to identify and compromise important nodes (CH nodes).

III IBS AND IBOOS FOR CWSNS

In this section, we introduce the IBS scheme and IBOOS scheme used in the paper. Note that the conventional schemes are not specifically designed for CWSNs. We adapt the conventional IBS scheme for CWSNs by distributing functions to different kinds of sensor nodes, based on at first. In order to further reduce the computational overhead in the signing and verification process of the IBS scheme, we adapt the conventional IBOOS scheme for CWSNs, based on.

3.1 Pairing for IBS

Boneh and Franklin [22] introduced the first functional and efficient ID-based encryption scheme based on bilinear pairings on elliptic curves. Specifically, randomly select two large primes p and q, and let E/Fp indicate an elliptic curve $y2 = x3+ax+b$ $(4a3 + 27b2 , 0)$ over a finite field Fp. We denote by G1 a q-order subgroup of the additive group of points in E/Fp, and G2 a q-order subgroup of the multiplicative group in the finite field $F* \ p$. The pairing is a mapping $e : G1 \times G1 \rightarrow G2$, which is a bilinear map with the following properties.

1) *Bilinear*

2) *Non-degeneracy*

3) *Computability*: There is an efficient algorithm tocompute

3.2 IBS Scheme for CWSNs

An IBS scheme implemented for CWSNs consists of the following operations, specifically, setup at the BS, key extraction and signature signing at the data sending nodes, and verification at the data receiving nodes.

• *Setup*: The BS (as a trust authority) generates a master key *msk* and public parameters *param* for the private key generator (PKG), and gives them to all sensor nodes.

• *Extraction*: Given an ID string, a sensor node generates a private key *sekID* associated with the ID using *msk*.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

• *Signature signing*: Given a message *M*, time-stamp *t* and a signing key _, the sending node generates a signature *SIG*.
• *Verification*: Given the *ID*, *M* and *SIG*, the receiving node outputs "accept" if *SIG* is valid, and outputs "reject" otherwise.

3.3 IBOOS Scheme for CWSNs

An IBOOS scheme implemented for CWSNs consists of following four operations, specifically, setup at the BS, key extraction and offline signing at the CHs, online signing at the data sending nodes, and verification at the receiving nodes.
• *Setup*: Same as that in the IBS scheme.
• *Extraction*: Same as that in the IBS scheme.
• *Offline signing*: Given public parameters and time-stamp*t*, the CH sensor node generates an offline signature *SIG* offline,and transmit it to the leaf nodes in its cluster.
• *Online signing*: From the private key *sekID*, *SIG*offline and message *M*, a sending node (leaf node) generates an online signature *SIG*online.

IVTHE PROPOSED SET-IBS PROTOCOL

In this paper, we propose two novel **S**ecure and **E**fficient data **T**ransmission (SET) protocols for CWSNs, called **SET-IBS** and **SET-IBOOS**, by using the **IBS** scheme and the **IBOOS** scheme, respectively. We first present SET-IBS in this section. The proposed SET-IBS has a protocol initialization prior to the network deployment and operates in rounds during communication, which consists of a setup phase and a steady-state phase in each round. We introduce the protocol initialization, describe the key management of the protocol by using the IBS scheme, and the protocol operations afterwards.

4.1 Protocol initialization

In SET-IBS, time is divided into successive time intervals as other LEACH-like protocols. We denote time-stamps by *Ts* for BS-to-node communication and by *t j* for leaf-to-CH communication. Note that key pre-distribution is an efficient method to improve communication security, which has been adapted in WSNs in the literature [8–10, 15–18, 29]. In this paper, we adopt *ID*||*t* as user's public key under an IBS scheme [24], and propose a novel secure data transmission protocol by using IBS specifically for CWSNs (SET-IBS). The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. In this way, when a sensor node wants to authenticate itself to another node, it does not have to obtain its private key at the beginning of a new round. Upon node revocation, the BS broadcasts the compromised node IDs to all sensor nodes, each node then stores the revoked IDs within the current round. We adopt the additively homomorphic encryption scheme in [30] to encrypt the plaintext of sensed data, in which a specific operation performed on the plaintext is equivalent to the operation performed on the cipher text. Using this scheme allows efficient aggregation of encrypted data at the CHs and the BS, which also guarantees data confidentiality. In the protocol initialization, the BS performs the following operations of key pre-distribution to all the sensor nodes.

4.2 Key management for security

Assume that a leaf sensor node *j* transmits a message *M* to itsCH *i*, and encrypts the data using the encryption key *k* from theadditively homomorphic encryption scheme [30]. We denotethe ciphertext of the encrypted message as *C*. We adapt thealgorithms of the IBS scheme from [24] to CWSNs practically and provide the full algorithm in the signature verification, where security is based on the DHP in the multiplicative group. The IBS scheme in the proposed SET-IBS consists of following three operations, extraction, signing and verification

4.3 Protocol operation

After the protocol initialization, SET-IBS operates in rounds during communication. Each round consists of a setup phase and a steady-state phase. We suppose that, all sensor nodes know the starting and ending time of each round, because of the time synchronization. Each round includes a setup phase for constructing clusters from CHs, and a steady-state phase for transmitting data from sensor nodes to the BS. In each round, the timeline is divided into consecutive time slots by the TDMA (time division multiple access) control [4]. Sensor nodes transmit

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

the sensed data to the CHs in each frame of the steady state phase. For fair energy consumption, nodes are randomly elected as CHs in each round, and other non-CH sensor nodes join clusters using one-hop transmission, depending on the highest received signal strength of CHs. In order to elect CHs in a new round, each sensor node determines a random number and compares it with a threshold. If the value is less than the threshold, the sensor node becomes a CH for the current round.

In this way, the new CHs are self-elected based by the sensor nodes themselves only on their local decisions, therefore, SETIBS functions without data transmission with each other in the CH rotations.

V THE PROPOSED SET-IBOOS PROTOCOL

We present the **S**ecure and **E**fficient data **T**ransmission (SET) protocol for CWSNs by using IBOOS (SET-IBOOS) in this section. The SET-IBOOS protocol is designed with the same purpose and scenarios for CWSNs with higher efficiency. The proposed SET-IBOOS operates similarly to the previous SETIBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication. We first introduce the protocol initialization, then describe the key management of the protocol by using the IBOOS scheme, and the protocol operations afterwards.

5.1 Protocol initialization

In order to reduce the computation and storage costs of signature signing processing in the IBS scheme, we improve SET-IBS by introducing IBOOS for security in SET-IBOOS. The operation of the protocol initialization in SET-IBOOS is similar to that of SET-IBS, however, the operations of key pre-distribution are revised for IBOOS. The BS does the following operations of key pre-distribution in the network:

• Generate an encryption key k for the homomorphic encryption scheme to encrypt data messages, where $k \in [m-1]$, m is a large integer.

• Let G be a multiplicative finite cyclic group with order q. The PKG selects a random generator g of group G generation, and chooses $\_ \in Z* q$ at random as the master key msk.

• For each node j, randomly select $r\,j \in Z* q$ for its private key generation, and let H be a hash function.

• Preload each sensor node j with the public parameters, given by $paramj=(k,m,G, q, g, \_, r\,j, H)$.

5.2 Key management for security

Assume that a leaf sensor node j transmits a message M to its CH i, and we denote the ciphertext of the encrypted message as Cj, which is encrypted by the same encryption scheme in SET-IBS. We adapt the algorithms from [21] to construct an IBOOS scheme for CWSNs, where security is based on the DLP in the multiplicative group. The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. The IBOOS scheme in the proposed SET-IBOOS consists of following four operations, extraction, offline signing, online signing and verification.

5.3 Protocol operation

The proposed SET-IBOOS operates similarly to that of SETIBS. SET-IBOOS works in rounds during communication, and the self-elected CHs are decided based on their local decisions, thus it functions without data transmission in the CH rotations.

VI PROTOCOL FEATURES

The protocol characteristics and hierarchical clustering solutions are presented in this section. We first summarize the features of the proposed SET-IBS and SET-IBOOS protocols as follows.

Both the proposed SET-IBS and SET-IBOOS protocols provide secure data transmission for CWSNs with concrete ID-based settings, which use ID information and digital signature for authentication. Thus, both SET-IBS and SET-IBOOS fully solve the orphan-node problem from using the symmetric key management for CWSNs.

• The proposed secure data transmission protocols are with concrete ID-based settings, which use ID information and digital signature for verification. Comparing the SETIBS, SET-IBOOS requires less energy for computation and storage. Moreover, the SET-IBOOS is more suitable for node-to-node communications in CWSNs, since the computation is lighter to be executed.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

• In SET-IBOOS, the offline signature is executed by the CH sensor nodes, thus, sensor nodes do not have to execute the offline algorithm before it wants to sign on a new message. Furthermore, the offline sign phase does not use any sensed data or secret information for signing. This is particularly useful for CWSNs, because leaf sensor nodes do not need auxiliary communication for renewing the offline signature.

6.1 Protocol Characteristics

In this part, we summarize the characteristics of the proposed SET-IBS and SET-IBOOS protocols. Table IV shows a general summary of comparison of the characteristics of SET-IBS and SET-IBOOS with prior ones, in which metrics are used to evaluate whether a security protocol is appropriate for CWSNs. We explain each metric as follows.

Key management: the key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric key based security.

• *Neighborhood authentication*: used for secure access and data transmission to nearby sensor nodes, by authenticating with each other. Here, "limited" means the probability of neighborhood authentication, where only the nodes with the shared pairwise key can authenticate each other.

• *Storage cost*: represents the requirement of the security keys stored in sensor node's memory.

• *Network scalability*: indicates whether a security protocol is able to scale without compromising the security requirements. Here, "comparative low" means that, compared with SET-IBS and SET-IBOOS, in the secure data transmission with a symmetric key management, the larger network scale. increases, the more orphan nodes appear in the network, and vice versa.

• *Communication overhead*: the security overhead in the data packets during communication.

• *Computational overhead*: the energy cost and computation efficiency on the generation and verification of the certificates or signatures for security.

• *Attack resilience*: the types of attacks that security protocol can protect against.

6.2 Secure Data Transmission with Hierarchical Clustering

In large scale CWSNs, multi-hop data transmission is used for transmission between the CHs to the BS, where the direct communication is not possible due to the distance or obstacles between them. The version of the proposed SET-IBS and SETIBOOS

protocols for CWSNs can be extended using multi-hop routing algorithms, to form secure data transmission protocols for hierarchical clusters. The solutions to this extension could be achieved by applying the following two routing models.

1) The multi-hop planar model: A CH node transmits data to the BS by forwarding its data to its neighbor nodes, in turn the data is sent to the BS. We have proposed an energy efficient routing algorithm for hierarchically clustered WSNs in [31], and it is suitable for the proposed secure data transmission protocols.

2) The cluster-based hierarchical method: The network is broken into clustered layers, and the data packages travel from a lower cluster head to a higher one, in turn to the BS,

VII PROTOCOL EVALUATION

In this section, we first introduce the three attack models of the adversaries, and provide the security analysis of the proposed protocols against these attacks. We then present results obtained from calculations and simulations. For the network simulations, we use the network simulator OMNeT++ 3.0 [33] to simulate SET-IBS and SET-IBOOS, and we focus on the energy consumption spent on message propagation and computation.

7.1 Security Analysis

In order to evaluate the security of the proposed protocols, we have to investigate the attack models in WSNs which threaten the proposed protocols, and the cases when an adversary (attacker) exists in the network. Afterwards, we detail the solutions and countermeasures of the proposed protocols, against various adversaries and attacks.

7.1.1 Attack Models

In this paper, we group attack models into three categories according to their attacking means as

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

follows, and study how these attacks may be applied to affect the proposed protocols.

• *Passive attack on wireless channel*: Passive attackers are able to perform eavesdropping at any point of the network, or even the whole communication of the network. Thus, they can undertake traffic analysis or statistical analysis based on the monitored or eavesdropped messages.

• *Active attack on wireless channel*: Active attackers have greater ability than passive adversaries, which can tamper with the wireless channels. Therefore, the attackers can forge, reply and modify messages.

• *Node compromising attack*: Node compromising Attackers are the most powerful adversaries against the proposed protocols as we considered. The attackers also can change the inner state and behavior of the compromised sensor node, whose actions may be varied from the premier protocol specifications.

7.1.2 Solutions to Attacks and Adversaries

The proposed SET-IBS and SET-IBOOS provide different types of security services to the communication for CWSNs, in both setup phase and steady-state phase.

Solutions to passive attacks on wireless channel: In the proposed SET-IBS and SET-IBOOS, the sensed data is encrypted by the homomorphic encryption scheme from [30],which deals with eavesdropping.

Solutions to active attacks on wireless channel: Focusing on the resilience against certain attacks to CWSNs mentioned in attack models, SET-IBS and SET-IBOOS work well against active attacks. Most kinds of attacks are pointed to CHs of acting as intermediary nodes, because of the limited functions by the leaf nodes in a cluster-based architecture.

Solutions to node compromising attacks: In case of attacks from a node compromising attacker, the compromised sensor node cannot be trusted anymore to fulfil the security requirements by key managements

7.2 Message Size of Data Transmission

In this part, we do the quantitative calculation of the message packet size on data transmission in the steady-state (main phase) of the different protocols for comparison

7.3 Simulation Results

Comprehending the extra energy consumption by the auxiliary security overhead and prolonging the network lifetime are essential in the proposed SET-IBS and SET-IBOOS. In order to evaluate the energy consumption of the computational overhead for security in communication, we consider three metrics for the performance evaluation: *Network lifetime*, *system energy consumption* and *the number of alive nodes*. For the performance evaluation,

• *Network lifetime* (the time of FND) - We use the most general metric in this paper, the time of FND (first node dies), which indicates the duration that the sensor network is fully functional.

The number of alive nodes - The ability of sensing and collecting information in a WSN depends on the set of alive nodes (nodes that have not failed). Therefore, we evaluate the functionality of the WSN depending on counting the number of alive nodes in the network.

• *Total system energy consumption* - It refers to the amount of energy consumed in a WSN. We evaluate the variation of energy consumption in secure data transmission protocols.

Node initial energy E_{init}	$1J$
Energy consumption on data aggregation E_{aggr}	$5nJ/bit$
Energy consumption on transmission amplifier E_{amp}	$100pJ/bit/m^2$
Energy consumption on signature signing and verification for SET-IBS E_{sig}	$77.4\mu J/signature$
Energy consumption on offline signature generation for SET-IBOOS $E_{offline}$	$5\mu J/signature$
Energy consumption on online signature signing and verification for SET-IBOOS E_{online}	$12.37\mu J/signature$
Hop-wise energy consumption on sending messages E_{send}	$59.2\mu J/byte$
Hop-wise energy consumption on receiving messages $E_{receive}$	$28.6\mu J/byte$

TABLE V: Parameter settings for the energy consumption in simulations

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

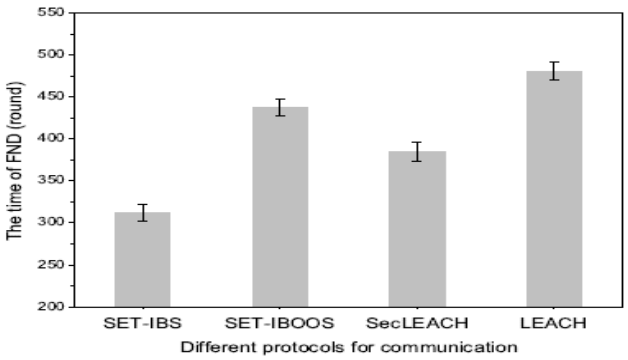
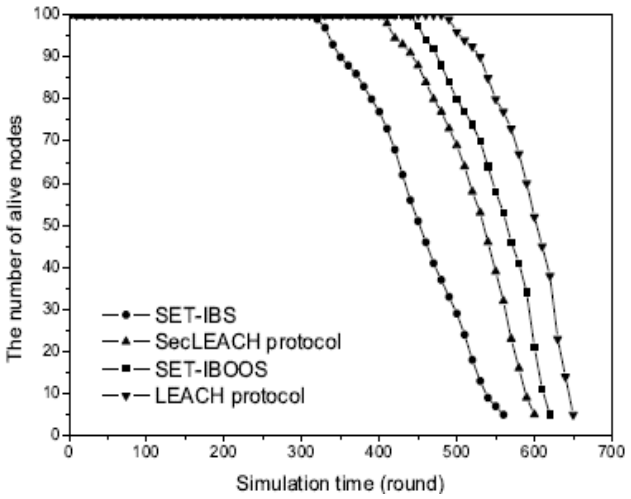


Figure 4: illustrates the time of FND using different protocols. We apply confidence intervals to the



simulation results, and a certain percentage (confidence level) is set to 90%

Fig. 6. Comparison of the number of alive nodes in different protocols

Figure 6 shows the comparison of system lifetime using SETIBS and SET-IBOOS versus LEACH protocol and SecLEACH protocol. The simulation results demonstrate that the system lifetime of SET-IBOOS is longer than that of SET-IBS and SecLEACH protocol. The time of FND in both SET-IBS and SET-IBOOS is shorter than that of LEACH protocol due to the security overhead on computation cost of the IBS process

VIII CONCLUSION

In this paper, we first reviewed the data transmission issues and the security issues in CWSNs. The deficiency of the symmetric key management for secure data transmission has been discussed. We then presented two secure and efficient data transmission protocols respectively for CWSNs, SET-IBS and SET-IBOOS. In the evaluation section, we provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SET-IBOOS are efficient in communication and applying the ID-based crypto-system, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management. Lastly, the comparison in the calculation and simulation results show that, the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computation and communication costs, we pointed out the merits that, using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.

REFERENCES

[1] T. Hara, V. I. Zadorozhny, and E. Buchmann, *Wireless Sensor Network Technologies for the Information Explosion Era*, *Stud. Comput. Intell.* Springer-Verlag, 2010, vol. 278.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2–23, 2006.

[3] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 14-15, pp. 2826–2841, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, 2002.

[5] A. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," *IEEE Trans. Parallel Distrib. Syst.*, vol. 13, pp. 1290–1302, 2002.

[6] S. Yi, J. Heo, Y. Cho *et al.*, "PEACH: Power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 14-15, pp. 2842–2852, 2007.