Volume 1, Issue 9, December 2016 ISSN: 2456-0006
International Journal of Science Technology Management and Research
Available online at: www.ijstmr.com

Digital Signature Based Secure Data Transmission for Cluster WSN

Ms. Gauri P.Heda
Dept. of Computer
S.N.D.C.O.R.C,Yeola,Dist-Nashik
Maharashtra, India

Prof. Imran R. Shaikh
Dept. of Computer
S.N.D.C.O.R.C, Yeola,Dist-Nashik
Maharashtra, India

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***.

Keywords: Cluster-based WSNs, ID-based digital signature, ID-based online/offline digital signature, secure data transmission Protocol.

I. INTRODUCTION

Recent development in the field of miniaturization led to the development of small tiny sensor nodes which can be deployed on various locations for achieving certain goals. The sensors are capable of self organizing themselves to form a network. Sensors are randomly deployed in the area of interest. As the devices are very small and inexpensive, they can be deployed in large numbers for better accurate sensing. They monitor conditions at different locations such as temperature, humidity, pressure, vehicular movement, soil makeup, lightning condition, noise levels, the presence or absence of certain kind of object etc.

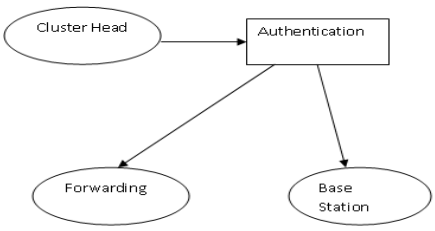


Fig 1: Authentication

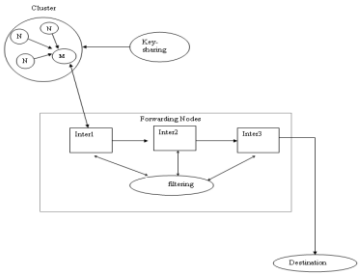


Fig 2: Formation of Cluster

A.Architecture of Clustering

Cluster-based data transmission in WSNs has been investigated by researchers to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes [3]. In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as cluster head (CH). A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to

the base station (BS). In Wireless Sensor Network the clustering is achieved for Network Scalability and Management which increase the lifetime of the sensor node and reduces the energy consumption. In the clustered Wireless Sensor Network, every cluster has a Cluster Head (CH) and the remaining nodes in the cluster are Leaf Nodes (Non Cluster Head Sensor Node), the data aggregated by the Leaf Node (Non Cluster Head Sensor Nodes) sends to the Cluster Head (CH) and the Cluster Head (CH) then transmits the data to the Base Station. The Low Energy Adaptive Cluster Hierarchy (LEACH) is most probably used for Low Energy Consumption of sensor node in Wireless Sensor Network. To avoid the quick energy consumption of CH's the LEACH protocol will randomly rotates the CH's among the sensor nodes which will leads to improving the Network lifetime. The Protocols which are similar to LEACH are APTEEN and PEACH.

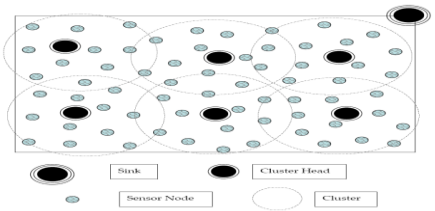


Fig 3: Architecture of a Hierarchical Network

B.Secure Data Transmission with Hierarchical Clustering

In large-scale CWSNs, multihop data transmission is used for transmission between the CHs to the BS, The version of the proposed SET-IBS and SET-IBOOS protocols for CWSNs can be extended using multihop 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: The multihop planar model. A CH node transmits data to the BS by forwarding its data to its neighbor nodes, in turn the data are sent to the BS. We have proposed an energy-efficient routing algorithm for hierarchically clustered WSNs, and it is suitable for the proposed secure data transmission protocols. 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, for example.

C.Auditing Technique

Security monitoring on the network is important, because computers sharing data are most readily available to an attacker. Without mechanisms in place to detect attacks as they occur, an system may not realize its security. Therefore it is vitally important that computers residing in the network are carefully monitored for a wide range of audit events. The auditing in a system consist of four steps. The first step is the attack has attempted on any node in system , secondly the attack is detected by the system by hashing algorithm after detection of attack the notifications are send to both producers and consumers and message is resend. Lastly the attack is prevented means no attack will happen again on same node by the same imp address. Due to this security is improved. The auditing takes place in a system in following way,

1. Attack:
The attacker tries to attempt attack on any node in a system. Once the attacker comes to know the imp address of consumer node, he will attack on that node and replaces the recent original message by his own message. Hence in this way the attacker make attack on nodes.

2. Attack Detection:
The system detects the attack attempted on nodes in a network. The detection of attacks done by auditing. The hashing value is created by the system for original message and also for attacker message. Both hashing values are compared and if the change has been found than the attack is detected by the system. The system comes to know the about the attack.

3. Notification
After detection of attack, the systems sends notification to nodes about attack. The
system notify to consumer that " There is attack by an ipa.b.c.d " which makes the
consumer alert. Also the system sends notification to producer that "a.b.c.d has made attack on the ipw.x.y.z. , please resend message" . Hence this will notify producer that he has to send the message to ipw.x.y.z again. Hence notifying improves the data integrity.

4. Attack Prevention :
For preserving the data integrity, it is very important to prevent the system from attack. After detecting the attack the system saves the imp address of the attacker and it will pre-vent the further attack by not allowing the node to receive message again from attacker padres. Hence attacker will not again able to attack on that nodes again once attempted. Hence, this is preventing our system from attack and improves security and data integrity. Hashing Algorithm : Most of the information security applications are sing Hash functions. A hash function is a scientific function that translates arithmetical input value to another compressed arithmetical value. The input to the hash function is always message

having arbitrary length but output is always a Hash value of fixed length. The value which we get as a final output is called as hash value because of hashing function applied over and sometimes it is also called as a message digest. For auditing, we arousing SHA1 hashing technique as an elementary operation as it can be replaced easily with the other cryptographic hash function like SHA2.

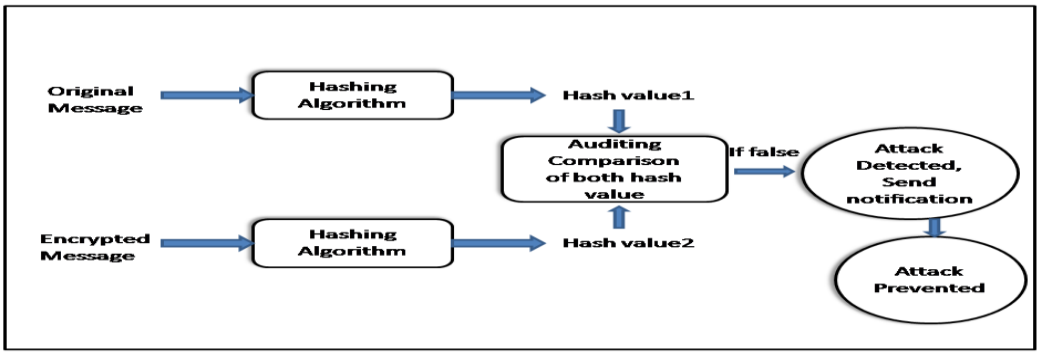


Fig4: Auditing Technique

II. RELATED WORK

The low-energy adaptive clustering hierarchy (LEACH) protocol presented by Heinzelman et al. [4] is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. To prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime. Following the idea of LEACH, a number of protocols have been presented such as APTEEN [5] and PEACH [6], which use similar concepts of LEACH. In this paper, for convenience, we call this sort of cluster-based protocols as LEACH-like protocols.

Routing Protocol In WSN	LEACH	TEEN	APTEEN	PEGASIS
Classification	Hierarchical			
Data Delivery	Cluster Head	Active Threshold	Active Threshold	Chain Based
Data Collection	Yes	Yes	Yes	No
Power consumption	High	High	High	Max
Scalability	Good	Good	Good	Chain Based
Overhead	High	High	High	Low
Network Life time	Very Good	Good	Good	Good
Resource Availability	Yes	Yes	Yes	Yes
Mobility	Fixed BS	Fixed BS	Fixed BS	Fixed BS

Table1: Comparison of different hierarchical protocol in WSN

III. LITERATURE SURVEY

A. Paper Title: Balanced energy sleep scheduling scheme for high density cluster-based sensor networks.
This in paper the concept analyzed as, Conserving Battery power in sensor network is an important aspect , to achieve this nodes which are ideal can be put to sleep so that the energy can be used only those nodes which are active [2] . Three scheduling schemes can be used, which are Balanced-energy scheduling scheme (BS), Randomized scheduling scheme (RS), Distance Based scheme (DS). Randomized Scheduling scheme (RS) selects the nodes randomly, which are ideal and puts them to sleep. Distance based scheduling scheme (DS) selects the ideal nodes with respect to the distance of those nodes from the cluster head. Balance-energy scheduling scheme maintains the average energy consumption of all the nodes in the cluster to be same. The BS is as same as DS..

B. Paper Title: Routing Techniques in Wireless Sensor Networks: A Survey
Clustering could reduce the energy consumption to some extent. Another method to reduce the energy-consumption is using Routing techniques. The data sensed by the sensor nodes are routed to the base station by some strategy which will reduce the energy consumption to a great extent. Routing in Wireless Sensor Network has three classification and they are

- Flat-based routing - all the nodes have equal functionality in the network
- Hierarchical-based routing - nodes have different functionality in the network
- Location-based routing - position of the nodes in the network decides the functionality.

In all the above routing techniques the best path that consumes less energy for the data transmission than any other path in the network is found and data is sent through it. If any node in the founded path is damaged or failed then the routing algorithm itself should accommodate a new path to the base station.

C. *Paper Title: Secure Routing In Wireless Sensor Networks: Attacks and Countermeasures*

Many routing protocols have been proposed to reduce the energy consumption in the network. But none of them had concerned with the security issues in the wireless sensor network [9]. If a Wireless sensor network is attacked, then it would cause a serious loss than any other network. The two classes of attacks against the sensor networks are sinkholes and Hello floods.

 Sinkhole Attack – It compromises a node in the network, attracts the neighboring nodes and makes every data to go through it with respect to the routing algorithm.

 Countermeasure – Geographic protocol is used to avoid sinkhole attack. This protocol uses the localized interaction and information to construct a topology and also avoid the initiation from the base station.

 Hello Flood attack – An attacker outside the network who has large transmission power may send a HELLO packet to every node in the network and them to believe that it is within the network. So, attacker can easily steal the data. Countermeasure - Each node is provided with an ID. And during data transmission each node should authenticate its neighboring node using Identity verification protocol to avoid Hello Flood attack. Multipath protocol can be used to avoid compromised nodes. In this protocol the data is routed over 'n' paths and the nodes in it are disjoint.

D. Paper Title: A Survey of Security Issues in Wireless Sensor Networks

This paper analyzes the efficiency of the Wireless sensor networks which are mainly used for military purpose for - send and receive the code or message [3] . It rectifies the open research issues for direction on security in WSNs. Secure routing protocols are be considered in key distribution the node sends the message from one node to base station. Aggregation of sensor data is to be secured.

IV. PROPOSED SYSTEM

We propose two Secure and Efficient data transmission protocols for CWSNs, called SET-IBS and SET-IBOOS. it provide 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 cryptosystem, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management.

A .Protocol Initialization

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; The BS does the following operations of key predistribution in the network: Generate an encryption key k for the homomorphic encryption scheme to encrypt data messages, where k € =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 *r* € Zq at random as the master key msk. For each node j, randomly select rj € Zq for its private k generation, and let H be a hash function .

B.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 SET-IBS, 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.

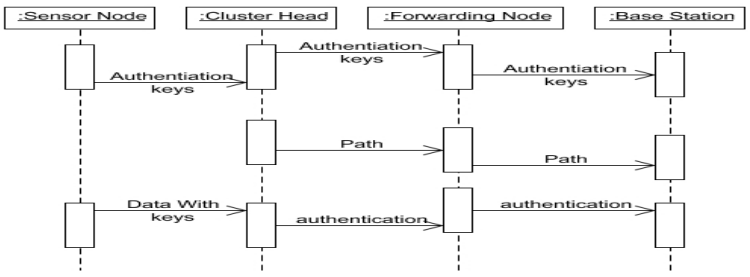


Fig 5: Architecture of Proposed System

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.

C.Protocol Characteristic:

The key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric keybased 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, "comparatively 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 [2].

V. ALGORITHMIC STUDY

- **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 first. To further reduce the computational overhead in the signing and verification process of the IBS scheme, we adapt the conventional IBOOS scheme for CWSNs.

A.Pairing for IBS

For self-contained, we briefly review the characteristics of pairing. Boneh and Franklin 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 $y2 = x3 + ax + b$ $(4a3 + 27b2 \neq 0)$ 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 Fp. The pairing is a mapping e : G1 × G2 □□G2, which is a bilinear map with the following properties:

1. Bilinear. P, Q, R, S € G1, e (P + Q , R + S) = e(P,R) e(P,S) e(Q,R) e(Q,S).
2. Nondegeneracy. If P is a generator of G1, then e(P;P) is a generator of G2.
3. Computability. There is an efficient algorithm to compute e(P,Q) in G2, P,Q G1.

The security in the IBS scheme is based on the bilinear Diffie-Hellman Problem (DHP) in the pairing domain [13], and the hardness of DHP is defined. A bilinear map e is secure if, given g; G;H € G1, it is hard to find h € G1 such that e(h,H) = e(g,G). Weil pairing and Tate pairing are the examples of such bilinear mapping, which present comprehensive descriptions of how pairing parameters can be selected for security.

B. IBS Scheme for CWSNs

1.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.

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

3.Signature signing. Given a message M, time stamp t and a signing key _, the sending node generates a signature SIG.

4. Verification. Given the ID, M, and SIG, the receiving node outputs "accept" if SIG is valid, and outputs "reject otherwise.

C. 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:

1.Setup. Same as that in the IBS scheme.

2.Extraction. Same as that in the IBS scheme.

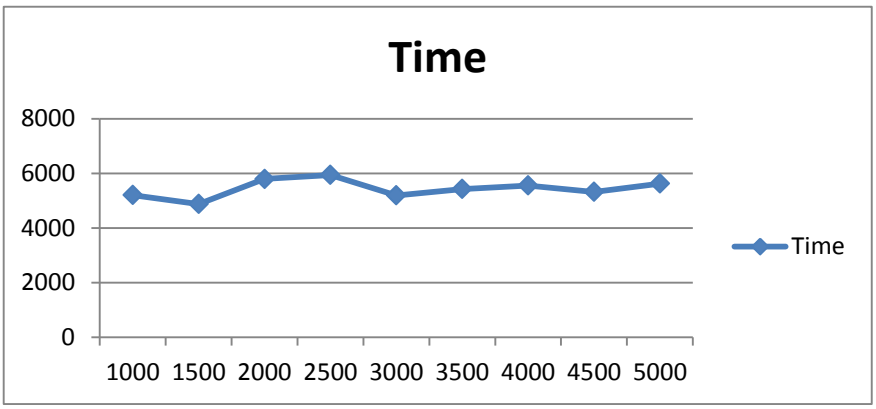
3.Offline signing. Given public parameters and time stamp t, the CH sensor node generates an offline signature SIGoffline, and transmit it to the leaf nodes in its cluster.

4.Online signing. From the private key sekID, SIGoffline and message M, a sending node (leaf node) generates an online signature SIGonline.

5. Verification. Given ID, M, and SIGonline, the receiving node (CH node) outputs "accept" if SIGonline is valid, and outputs "reject" otherwise

VI. RESULTS

A.Amount of Time

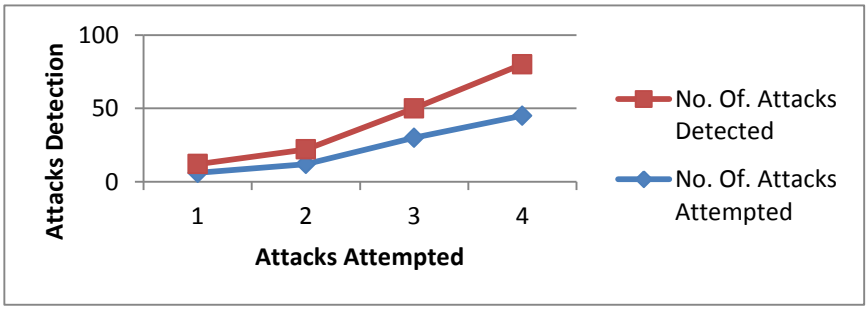


Graph 1: Amount of time

Message size(bytes)	Time
1000	5204
1500	4879
2000	5796
2500	5940
3000	5194
3500	5428
4000	5558
4500	5322
5000	5625

Table2: Table for Graph

B. Attack Detection:

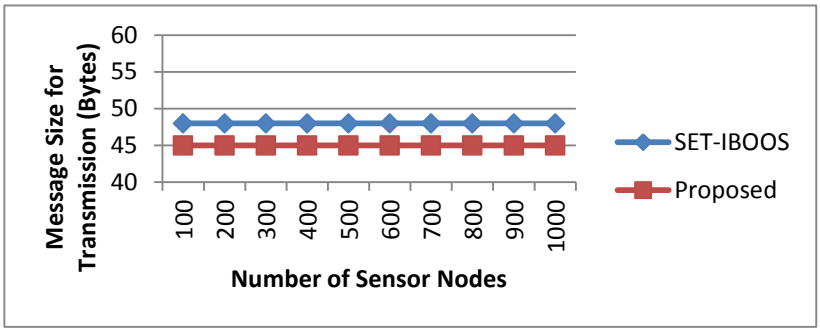


Graph2: Attack Detection

Number	No. Of. Attacks Attempted	No. Of. Attacks Detected
1	6	6
2	12	10
3	30	20
4	45	35

Table 3: Table for Graph

C. Number of Sensor Node



Graph 3: Number of Sensor Node

The total message sizes in different protocols for data transmission, which achieve a similar security level to RSA-1024, by concerning the number of sensor nodes. Wean see that the proposed set has smaller message size than SET IBOOS protocol.

	SET-IBOOS	Proposed
100	48	45
200	48	45
300	48	45
400	48	45
500	48	45
600	48	45
700	48	45
800	48	45
900	48	45
1000	48	45

Table 4: Table of Graph

CONCLUSION AND FUTURE WORK

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 SETIBOOS are efficient in communication and applying the IDbased cryptosystem, 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.

REFERENCE

1. I.F Akylidiz, "Wireless Sensor Networks a survey", Computer Networks 38(2009)
2. C-Y Chong, S.P Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges", Proceedings of the IEEE 91 (8) (2003)
3. D. Estrin, "Next century challenges: Scalable coordination in sensor Network", in: Proceedings of the Fifth International Conference on Mobile Computing and Networks (MobiCom „99)
4. 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.
5. 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.
6. Mohamed Younis, Moustafa Youssef, Khaled Arisha, "Energy-Aware Routing in Cluster-Based Sensor Networks".
7 . Jamal N. Al-Karaki, The Hashemite University Ahmed E. Kamal, Iowa State University "Routing Techniques "
8. L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.
9. P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks," Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA), pp. 145-152, 2007.
10. K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM), pp. 1-5, 2008.
11. S. Sharma and S.K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," Proc. Int'l Conf. Comm., Computing & Security (ICCCS), pp. 146-151, 2011.
12. G. Gaubatz et al., "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," Proc. IEEE Third Int'l Conf. Pervasive Computing and Comm. Workshops (PerCom), pp. 146-150, 2005.