International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.4, No.1, January 2015 DOI:10.15693/ijaist/2015.v4i2.330-337

Energy Aware and Secured Cluster Based Wireless Sensor Network

P.Narayini
Assitant Professor/Department of ECE
UCETW, Madurai, India

I.Reshma Grace
Student/Department of ECE
UCETW, Madurai, India

M.S.Subhashini
Student/Department of ECE
UCETW, Madurai, India

K.Vidhyaa
Student/Department of ECE
UCETW, Madurai, India

***Abstract*—Secure data transmission is a critical issue for wireless sensor networs. Sensor node normally senses the physical events such as temperature, sound, vibration, pressure etc. Each node has its internal memory to store the information regarding the transmitting data.This data finally reaches to the base station. The data which sensor node transmitshould be secret or confidential for the application. To obtain secure communication between intermediate nodes as well as the base station hashingtechnique is proposed instead of SET-IBS and SET-IBOOS. The main concept in these protocols are to secure the sensed data. For efficient communication key management and cluster formation is implemented. For encrypt the parameter of the sensed data to be encrypted by homomorphic encryption scheme and ID-based cryptosystem. In SET-identity-based digital signature scheme consists of three operation such as extraction, signing, and verification but in SET-IBOOS there are extraction, offline signing, online signing, and verification operation will be implemented. But security is considered to be higher in SET-IBOOS than SET-IBS.**

***Index terms* -ID-based digital signature,ID-based online/offline digital signature,secure data transmission protocol.**

I.INTRODUCTION

In Most Wireless Sensor Network applications, the entire network must have the ability to operate in harsh environments regardless of the constraints. The Basic feature of any sensor networks is to monitor and sense the surrounding. Catastrophic conditions can be expected due to the short duration of the battery energy of the sensors and the possibility of damaged nodes during deployment as the large number of sensors is expected .This leads to Obstacles in Sensor Security in major ratio. Hence Data confidentiality and authentication is taken into consideration.

The need for Clustering in Wireless Sensor Networks is first motivated where data transmission can be efficiently managed. Naturally grouping of sensor nodes into clusters has been widely adopted to satisfy scalability, high energy efficiency and prolonged network life span in abundance. The corresponding data gathering protocols imply cluster organization of the sensors which makes possible for data fusion and aggregation, thus leading to significantenergy savings. The Cluster formation process leads to Cluster Head (CH) nodes and non-CH nodes. The CH node collects the sensed data from all other non-CH nodes (Leaf Nodes) for data transmission and transmits them across the networks. In Clustering Scheme, the nodes are divided into groups mostly based on geographical location. Each group contains a single Cluster Head and several other ordinary nodes (leaf nodes). It performs intra-cluster transmission arrangement, data aggregation and forwarding. The Base station(BS) is considered as the data processing unit for the data received from the sensors and the data accessed by the end users. The main objectives show cases that the Base station generates a master key (Common Key Parameter) and distributes it to all other sensor nodes. Meanwhile the other non-CH nodes(leaf nodes) with its own private key and the Master key given by the Base station forwards to its CH node .The sender node has a signature of encrypted message, MAC address and receiver node Id. Based on the set up we can choose any of the two proposed protocols.

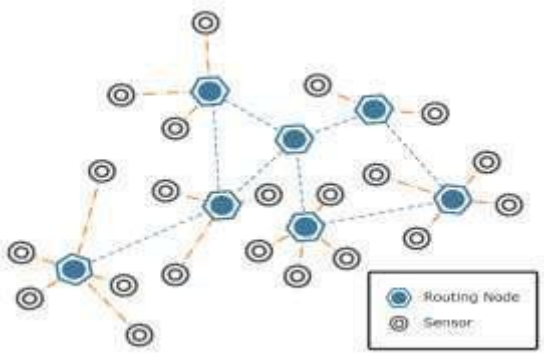


Fig.1.Nodes in sensor network

In SET-IBS protocol, we can able to detect the attack scenario only once the message has reached to its destination node. In

SET-IBOOS protocol, we can detect the attack at its early stage by considering time parameter and loss of energy consumed. If there is delay of message content at its destination node, then this signifies that the attack has taken place. There is also possibility of modifying the content of the message. These two protocols greatly contribute in identifying the threat by making use of Digital Signature. Hence considering the existing cluster based Wireless Sensor Network protocols like LEACH (Low Energy Adaptive Clustering Hierarchy), SET-IBS and SET-IBOOS protocols have proved its feasibility enhancement in terms of energy ration and transmission overhead.

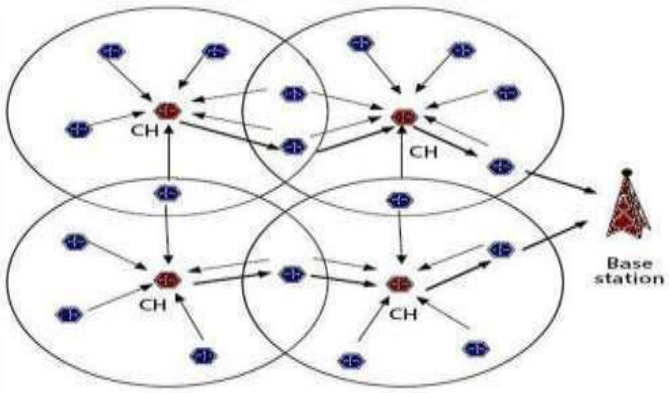


Fig.2. Data Communication in Cluster Based Wireless Sensor Networks

II. PROBLEM STATEMENT

A. Design Methodology

Consider the system design as shown in the Fig.1 depicting the clustering mechanism. Here the BS acts as a trusted authority and distributes the master key to all other leaf nodes (non-CH nodes).The CH node collects all the data from the non-CH nodes and sends the same to receiver node or else to the BS. An approximate amount of energy is consumed during data communication and data processing. Data transmission costs more as compared to other roles and therefore CH node plays an important role in the transmission.

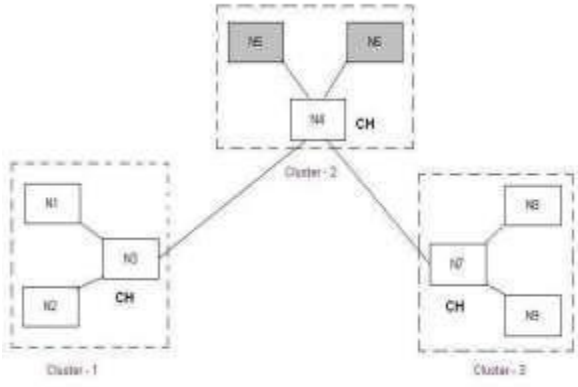


Fig.3.System Design Architecture

In the existing design architecture the message data is not encrypted before sending it to other nodes in the clusters. Moreover WSN's have many unconnected nodes termed as orphan nodes which generally fails to obtain the network address from a parent node. The large number of orphan nodes adversely affects the performance of WSN application. In this paper, the proposed protocols SET-IBS and SET-IBOOS by using Paillier Encryption technique resolves the problem statement. Digital Signature is considered as an Identity.

B. Vulnerabilities and Security threats

Security plays a major role in every aspect of WSN. During data transmission there can be chances of replacing the message, modifying the content, pretending to be a CH node etc. This ultimately results into major security assets. In this paper we can able to track content modification attack, time delay attack and no attack scenarios.

C.Content Modification Attack

In this mode, a message data is transmitted from sender node to the destination node. By using Digital Signature as an Identity it is possible to make out the modified message.

D.Time Delay Attack

In this mode, by using time parameter we can able to identify that the message has been modified. The time parameter is already predefined. If the message reaches within the stipulated time then it confirms that there is no attack. On the other hand, if the message could not able to make it in the stipulated time then it confirms that there is an attack.

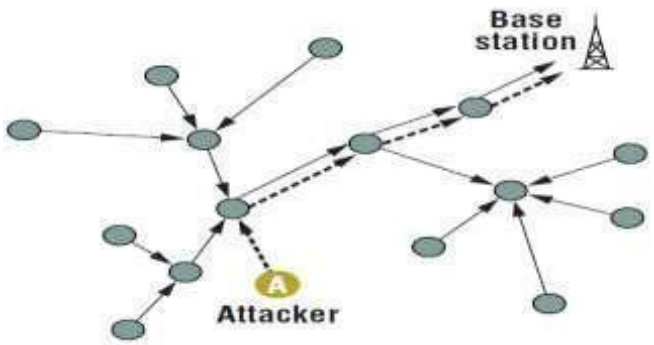


Fig.4.Attackers in sensor network

III.DESIGNATION SEQUENCED DISTANCE VECTOR ROUTING PROTOCOL

Destination sequenced distance vector routing (DSDV) is adapted from the conventional Routing Information Protocol (RIP) to ad hoc networks routing. It adds a new attribute, sequence number, to each route table entry of the conventional RIP. Using the newly added sequence number, the mobile nodes can distinguish stale route information from the new and thus prevent the formation of routing loops.

A.Packet Routing And Routing Table Management

In DSDV, each mobile node of an ad hoc network maintains a routing table, which lists all available destinations, the metric and next hop to each destination and a sequence number generated by the destination node. Using such routing table stored in each mobile node, the packets are transmitted between the nodes of an ad hoc network. Each node of the ad hoc network updates the routing table with advertisement periodically or when significant new information is available to maintain the consistency of the routing table with the dynamically changing topology of the ad hoc network.Periodically or immediately when network topology changes are detected, each mobile node advertises routing information using broadcasting or multicasting a routing table update packet. The update packet starts out with a metric of one to direct connected nodes. This indicates that each receiving neighbor is one metric (hop) away from the node. It is different from that of the conventional routing algorithms. After receiving the update packet, the neighbors update their routing table with incrementing the metric by one and retransmit the update packet to the corresponding neighbors of each of them. The process will be repeated until all the nodes in the ad hoc network have received a copy of the update packet with a corresponding metric. The update data is also kept for a while to wait for the arrival of the best route for each particular destination node in each node before updating its routing table and retransmitting the update packet. If a node receives multiple update packets for a same destination during the waiting time period, the routes with more recent sequence numbers are always preferred as the basis for packet forwarding decisions, but the routing information is not necessarily advertised immediately, if only the sequence numbers have been changed. If the update packets have the same sequence number with the same node, the update packet with the smallest metric will beused and the existing route will be discarded or stored as a less preferable route. In this case, the update packet will be propagated with the sequence number to all mobile nodes in the ad hoc network. The advertisement of routes that are about to change may be delayed until the best routes have been found. Delaying the advertisement of possibly unstable route can damp the fluctuations of the routing table and reduce the number of rebroadcasts of possible route entries that arrive with the same sequence number. The elements in the routing table of each mobile node change dynamically to keep consistency with dynamically changing topology of an ad hoc network. To reach this consistency, the routing information advertisement must be frequent or quick enough to ensure that each mobile node can almost always locate all the other mobile nodes in the dynamic ad hoc network. Upon the updated routing information, each node has to relay data packet to other nodes upon request in the dynamically created ad hoc network.

B.Evaluation of DSDV

Complexity

In DSDV, the time complexity is *O(d = network diameter)*,and the communication complexity (link addition/failure) is *O(N = number of nodes in thenetwork)*.

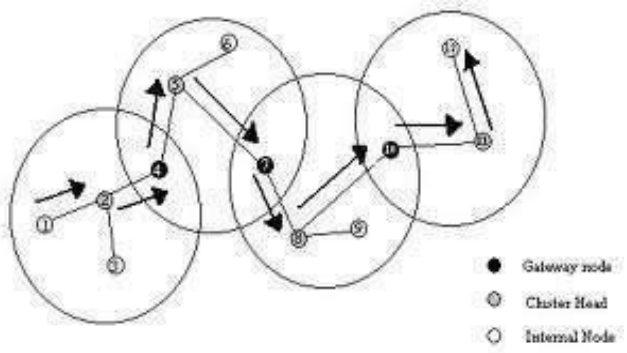


Fig.5. Protocol assignment

Performance

DSDV requires that each node maintain two tables. The bulk of the complexity in DSDV is generating and maintaining these tables. The updates are transmitted to neighbors periodically or scheduled as needed. As growing of mobility and number of nodes in the network, the size of the bandwidth and the routing tables required to update these tables grows simultaneously. The overhead for maintaining

and updating these tables will increase correspondingly.It is natural that heavy routing overhead will degrade the performance of the network.

Stability and scalability

DSDV guarantees loop-free routes in routing packets. It uses incremental and full dump for updates. The incremental update is used so that the entire routing table needs not to be transmitted for every change in the network topology. However, DSDV requires the full dump update periodically, regardless of the number of changes in the network topology. In this aspect, DSDV is not efficient in route updating. It also limits the number of nodes that can join in the network. In addition, whenever the topology of a network changes,DSDV is unstable until update packets propagate throughout the network

QoS Routing with DSDV

The requirements of QoS routing in a wireless network that supports multimedia traffic and/or interconnected to a wired ATM backbone were identified in.For general purpose, the requirements of QoS routing in ad hoc networks that support real time traffic are summarized here:

(1) *Band reservation*: The ad hoc network must allocate bandwidth at call setup time inorder to support real time connections.

(2) *QoSrouting*:To support QoS for real time traffic, the mobile nodes not only need to know the minimum delay path to destination but also need to have the knowledge of the bandwidth available on that path. At call setup time, the bandwidth has to be available and reserved. Otherwise the call setup request will be rejected. Thus, traditional distance vector routing algorithms are not adequate. Routing with QoS is required for efficiently managing bandwidth resources.

(3)*Congestion control*: Even though using QoS routing can manage the bandwidth resources at call setup time, network congestion due to the dynamics of mobility and of traffic patterns has to be controlled via applying selective packet dropping and input rate control, etc.

(4) *Mobility*: The inter-working of mobility as well as the allocation and maintenance of bandwidth resources are critical to an ad hoc network, especially when it interconnects to a wired backbone..

IV. WORKING PROCEDURE

SHA-1 Secure Hash Algorithm

SHA1 Description

SHA1 Description SHA 1 stands for "Secure Hashing. Algorithm" I t is a hashing algorithm designed by the United States National Security Agency and published by NIST. I t is the improvement upon the original SHA 0 and was first published in 1995. SHA 1 is currently the most widely used SHA hash function,although it will soon be replaced by the newer and potentially more secure SHA 2 family of hashing functions. I t is currently used in a wide variety of applications, including TLS, SSL, SSH and PGP.

SHA 1 outputs a 160-bi t digest of any sized fi le or input. I n construction i t is similar to the previous M D4 and M D5 hash functions, in fact sharing some of the initial hash values. I t uses a 512 bi t block size and has a maximum message size of bits.

SHA 1 Algorithm Description

- Padding
  - by
  - zeroes until the final block has 448 bits.

    Append the size of the original message as an unsigned 64 bit integer.
- Initialize the 5 hash blocks (h0, h1, h2, h3, h4) to the specific constants defined in the SHA 1 standard.
- Hash (for each 512-bi t Block) Padthemessagewithasingle one followed

  Allocate an 80 word array for the message schedule

  Set the first 16 words to be the 512-bi t block split into 16 words.

  The rest of the words are generated using the following algorithm word[i -3] XOR word[i -8] XOR word[i -14] XOR word[i -16] then rotated 1 bit to the left.
  - Loop 80 times doing the following. (Shown in I mage1)
    - Calculate SHA function () and the constant K (these are based on the current round number.
    -
    -
    - (rotated left 30)
-
  - (rotated left 5) + SHA function() + + word[i]
  - Add a, b, c, d and e to the hash output.

Output the concatenation (h0, h1, h2, h3, h4) which is the message digest.

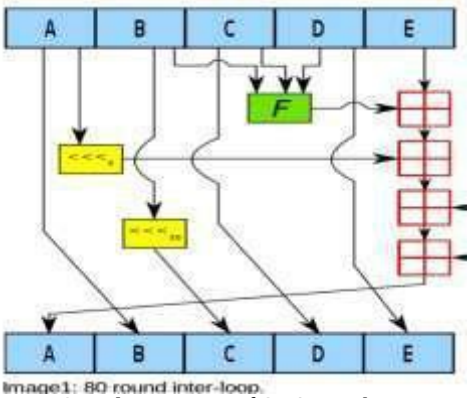


Fig.6.implementation of SHA-1 technique

Example Inputs and Outputs

Input (Text file)	Output(SHA1 Hash)
abcd	81fe8bfe87576c3ecb22426f8e57847382917acf
abcdefghijklmnopqrstuvwxyz	32d10c7b8cf96570ca04ce37f2a19d84240d3a89
The Quick Brown Fox Jumps Over The Lazy Dog	645218467886dd414ea66a09b6cceea806127fb5
The quick brown fox jumps over the lazy dog	2fd4e1c67a2d28fced849ee1bb76e7391b93eb12

V.DSA - DIGITAL SIGNATURE ALGORITHM

A.Key generation

Key generation has two phases. The first phase is a choice of algorithm parameters which may be shared between different users of the system, while the second phase computes public and private keys for a single user.

B.Parameter generation

- Choose an approved cryptographic hash function H. In the original DSS, H was always SHA-1, but the stronger SHA-2 hash functions are approved for use in the current DSS.The hash output may be truncated to the size of a key pair.
- Choose an N-bit prime q. N must be less than or equal to the hash output length.
- Choose an L-bit prime modulus p such that is a multiple of q.
- Choose g, a number whose multiplicative order modulo p is q. This may be done by setting for some arbitrary , and trying again with a different h if the result comes out as 1. Most choices of h will lead to a usable g; commonly is used.
- The algorithm parameters may be sharedbetween different users of the system

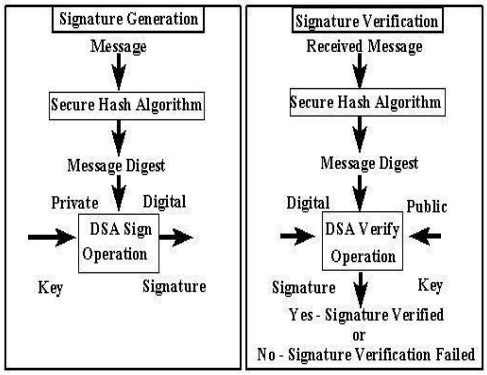


Fig.7.implementation of DSA

C.Per-user keys

Given a set of parameters, the second phase computes private and public keys for a single user:

- Choose *x* by some random method, where .
- Calculate .
- Public key is . Private key is *x*.

There exist efficient algorithms for computing the modular exponentiations and , such as exponentiation by squaring.

D.Signing

Let H be the hashing function and m the message:

- Generate a random per-message value k where
- Calculate
- In the unlikely case that , start again with a different random k
- Calculate .
- In the unlikely case that , start again with a different random k
- The signature is .

The first two steps amount to creating a new per-message key. The modular exponentiation here is the most computationally expensive part of the signing operation, and it may be computed before the message hash is known. The modular inverse is the second most expensive part, and it may also be computed before the message hash is known. It may be computed using the extended Euclidean algorithm or using Fermat's little theoremas .

E.Verifying

Reject the signature if or is not satisfied

- Calculate
- Calculate
- Calculate
- Calculate
- The signature is valid if .

F.Correctness of the algorithm

The signature scheme is correct in the sense that the verifier will always accept genuine signatures. This can be shown as follows:

First, if it follows that by Fermat's little theorem. Since and q is prime, g must have order q.

The signer computes

Thus
=

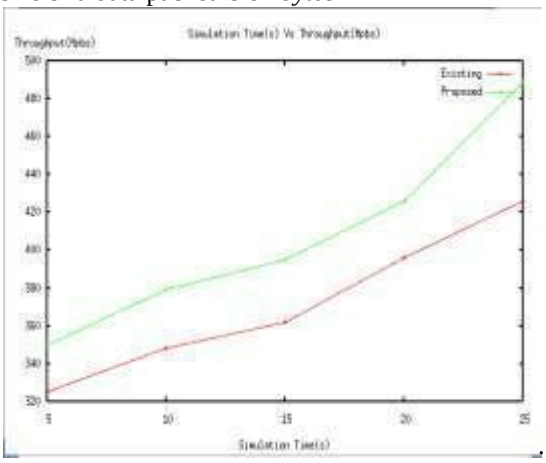
Since *g* has order we have

=
=

Finally, the correctness of DSA follows from

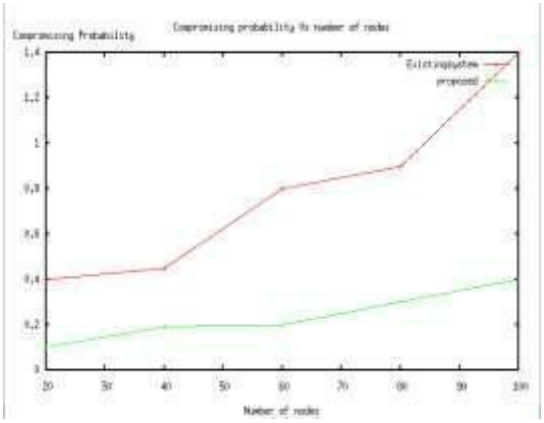
VI.Message Size Of Data Transmission

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. In the proposed SET-IBS, the message packet size on transmission for node *j* which equals to$|IDj| + |ti| + |C| + |\sigma j| + |h(C||ti||\theta)|$. $|h(C||ti||\theta)|$ is a hash value, which is 20 *bytes* when SHA-1 is used. Although most of existing WSNs constructedin real world use no more than 200 nodes a large scale WSN could consist of hundreds of nodes or more in the future. Thus in this paper, we set the length of a node ID as 2 *bytes*. In addition, the time stamp $|ti|$ is very small like 2 *bytes*, and $|C|$ is assumed as 20 *bytes*. The total message size of a transmission packet is $61 + |\sigma j|$ *bytes*, whereas, $|\sigma j|$ is variable which provides the currently accepted security level. Inthis way, the total message size of a data packet is 61 *bytes*



VII.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.



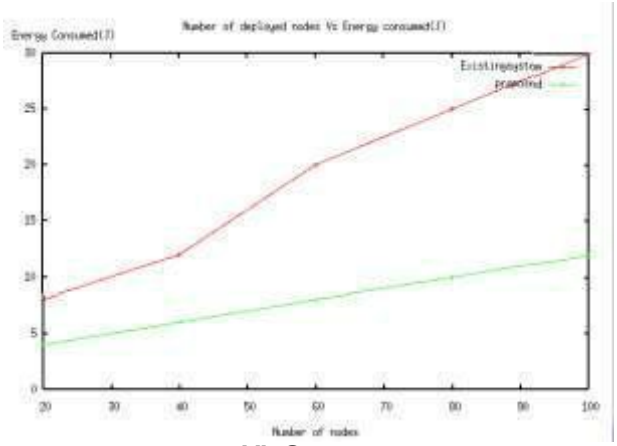
VIII.SIMULATION RESULTS

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 theperformance evaluation, we compare the proposed SET-IBSand SET-IBOOS with LEACH protocol and Sec LEACHprotocol.

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.Therefore, maximizing the time of FND in a WSN means to prolong the network lifetime.

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.



VI. CONCLUSION

We have proposed a new approach for message authentication in wireless sensor networks. The proposed scheme is based on modified SHA-1 hash function by using regularly distributed pseudo random function. The reliable MAC algorithm provides both message authenticity and integrity for unique messages. We analyzed security and efficiency of the proposed scheme. Additionally, we suggested two scenarios according to the number of sensor nodes. In future, this scheme can be extended to as an intrusion detection system to detect and reject maliciousnodes in wireless sensor networks by using MACs.

.

REFERENCES

[1] T. Hara, V. I. Zadorozhny, and E. Buchmann, *Wireless Sensor Network Technologies for the Info. 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, 2006.

[3] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 14-15, 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, 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, 2002.

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

[7] K. Pradeepa, W. R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," *Int. J. Comput. Applications*, vol. 47, no. 11, 2012.

[8] L. B. Oliveira, A. Ferreira, M. A. Vilac¸a*et al.*, "SecLEACH-On the security of clustered sensor networks," *Signal Process.*, vol. 87, 2007.

[9] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and performance analysis of a secure clustering protocol for sensor networks," in *Proc. IEEE NCA*, 2007.

[10] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," in *Proc. WiCOM*, 2008.

[11] S. Sharma and S. K. Jena, "A survey on secure hierarchical routing protocols in wireless sensor networks," in *Proc. ICCCS*, 2011.

[12] G. Gaubatz, J. P. Kaps, E. Ozturk*et al.*, "State of the Art in Ultra-Low Power Public Key Cryptography for WSNs," in *Proc. IEEE PerCom Workshops*, 2005.

[13] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in *Lect. Notes.Comput.Sc. - CRYPTO*, 2001.

[14] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Lect. Notes. Comput.Sc. - CRYPTO*, 1985.

[15] D. W. Carman, "New Directions in Sensor Network Key Management," *Int. J. Distrib. Sens. Netw.*, vol. 1, 2005.

[16] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures," in *Proc. IEEE CIT*, 2010.

[17] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based WSNs Using ID-Based Digital Signature," in *Proc. IEEE GLOBECOM*, 2010.

[18] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," in *Lect. Notes.Comput.Sc. - CRYPTO*, 1990.

[19] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," in *Lect. Notes.Comput. Sc. - Inf. Secur. Privacy*, 2006.

[20] C.-K. Chu, J. K. Liu, J. Zhou *et al.*, "Practical ID-based encryption for wireless sensor network," in *Proc. ACM ASIACCS*, 2010.

[21] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, 2003.

[22] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," in *Lect. Notes.Comput. Sc. - SAC*, 2003.

[23] J. Liu and J. Zhou, "An Efficient Identity-Based Online/Offline Encryption Scheme," in *Lect. Notes.Comput. Sc. - Appl. Crypto. Netw.Secur.*, 2009.
[24] J. J. Rotman, *An Introduction to the Theory of Groups*. Springer-Verlag; 4th edition, 1994.
[25] K. S. McCurley, "The discrete Logarithm Problem," in *Proc. Symp. Appl. Math.*, *Prog. Com. Sc.*, 1990, vol. 42.
[26] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, 1976.
[27] D. Boneh, I. Mironov, and V. Shoup, "A Secure Signature Scheme from Bilinear Maps," in *Lect. Notes.Comput. Sc. - CT-RSA*, 2003.
[28] P. Barreto, H. Kim, B. Lynn *et al.*, "Efficient Algorithms for Pairing-Based Cryptosystems," in *Lect. Notes.Comput.Sc. - CRYPTO*, 2002.
[29] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypteddata in wireless sensor networks.

Authors Profile

I.Reshma Grace currently doing **B.E.** degree in electronics and communication engineering from Ultra College of Engineering and Technology for Women, Madurai, Anna University, Chennai, India.Her area of interest includes wireless communication (**WiFi,WiMax**), Mobile Ad hoc networks ,Sensor Networks ,Neural Networks and fuzzy logic, Communication networks

M.S.Subhashini Currently doing **B.E.** in electronics and communication engineering in Ultra College of Engineering and Technology for Women, Madurai, Anna University,Chennai,India. His research interest includes wireless communication (**WiFi,WiMax**), Mobile Ad hoc networks ,Sensor Networks ,Neural Networks and fuzzy logic, Communication networks

K.Vidhyaa received the **B.E.** degree in electronics and communication engineering from the Ultre College of Engineering and Technology for Women, Madurai, Anna University, Chennai, India. Her research interest includes wireless communication (**WiFi,WiMax**), Mobile Ad hoc networks ,Sensor Networks ,Neural Networks and fuzzy logic, Communication networks.