Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NOVEL IDENTITY BASED CRYPTO LOGICAL APPROACH FOR CLUSTER EMPLOYED SECURE WIRELESS SENSOR NETWORKS

[1] A.JEGATHEESAN, [2] DR.D.MANIMEGALAI, [3] G.THANUSHA

[1]Asstt. Prof., Department of Information Technology, Cape Institute of Technology, Levengipuram,INDIA

[2]Prof., Department of Information Technology, National Engineering College, Kovilpatti, INDIA

3Asstt Prof., Department of Information Technology, Cape Institute of Technology, Levengipuram, INDIA

E-mail: [1]thanusha128@gmail.com, [2] jegatheese@gmail.com [3] megalai_nec@yahoo.co.in

ABSTRACT

Wireless sensor network (WSN) is a network system comprised of spatially distributed devices using wireless sensor nodes. Due to the resource-limited sensor nodes, customary network security mechanisms are not suitable for WSNs. In this paper, we present a security mechanism, in which along with Mote Sec an Identity-Based digital Signature (IBS) scheme is employed on the network layer for WSNs with focus on secure network protocol and data access control. The IBCLA scheme uses IBS as identifiers for a node in the network to ensure concealment of its true identifier (ID).IBCLA can be embedded into any Wireless Sensor Network (WSN) routing protocol to ensure anonymity and privacy during node discovery, routing and data delivery in the network. The scheme is mostly engaged for Cluster founded network therefore boost the security of the system. In the proposed protocols, BS initially distributed secure keys and public parameters to all sensor nodes, which overcomes the key escrow problem recounted in ID-based crypto-systems. Secure communication in Identity founded digital signature relies on the ID-based cryptography, in which, user public keys are their Identity information. Therefore, sensor nodes can get the corresponding personal keys without auxiliary data transmission, which is effective in connection and saves energy.

Keywords: *Wireless sensor network (WSN), Identity-Based digital signature, key escrow problem, secure network protocol, data access control*

1. INTRODUCTION

The wireless sensor network is composed of thousands to millions of small sensors form self-organizing wireless network. Security for sensor network is not easy. These sensors will have limited processing power, storage, bandwidth and energy. The wireless sensor networks have been widely used in many applications such as environmental, hospital, military, organizations and smart home. Due to their nature of wireless communication, highly constrained in term of resources, limited computational time and memory space the WSNs are more vulnerable to various attacks. The attacker can continuously send packet to drain node's batteries and waste network bandwidth, attacker can steal nodes, and pose unauthorized node in the network. In some application node authentication, packet authentication, packet confidentiality and packet integrity are more important. In this paper we present the secure wireless sensor network to provide secure network protocol, access control, security against node compromising and node capturing attacks.

Anonymity in wireless sensor networks used to prevent sender's and receiver's identity from third party. Anonymizing sensor nodes can confuse adversaries about which sensor is the real sender of a message. To protect the real ID of CH (Cluster Head), IBS can be used for CH instead of real ID. Misra *et al.*[1] proposed anonymous schemes for clustered wireless sensor networks.

For introducing several attacks, an attacker node initially compromises several sensor nodes and accesses all keying materials kept in the compromised nodes then controls these compromised nodes to inject false data and send those information to the sink to cause high-level error decision. Therefore, it is crucial to notice

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

compromised node as accurately as attainable in wireless sensor networks which results in energy deprivation.

A significant benefit one will occur from using public-key crypto logical algorithms for WSN security is that this simplifies essential security services together key distribution/management and hence reduces transmission power due to less protocol overhead. In a recent work, Wen Hu [2, 3] used the TPM hardware. It is based on Public

Key (PK) platform. One necessary issue that should be resolved in order to completely utilize public-key cryptography in WSN is to make up a public key infrastructure (PKI) for WSN, which is to establish a trust worthy identity. However the PKI for WSNs is not important to construct.

1.1 Contributions and Organization

The Identity Based Crypto Logical Approach (IBCLA), designed on the network layer for wireless sensor networks (WSNs) with concentrate on secure network protocol and access control [4]. The proposed protocols have better performance than existing secure protocol for WSNs, in terms of security overhead and energy consumption. The IBCLA provides the Identity-Based digital Signature to prevent the active and passive attacks on wireless channel, compromised node attack to achieve the goal of data access control to define access rights in cluster head node because of its characteristics low overhead.

Our main contributions are summarized as follows:

- The IBCLA method used to prevent compromised node attack and node capturing attacks.
- IBCLA is able to achieve the goals of much less energy consumption and higher security than previous works.

The rest of the paper is described as follows. The related works are given in Section 2. Section 3 describes the system model, including topology and attack model. In Section 4, we describe the details of the proposed method. Section 5 describes the metrics used to evaluate and analyze the performance for IBCLA. The conclusions are drawn in Section 6.

2. RELATED WORKS

The secure network protocol for wireless sensor networks is proposed in SPINS [5]. SPINS has two secure building blocks: SNEP and TESLA. SNEP provides the information confidentiality, two-party information authentication, and data freshness. TESLA is a new protocol which provides authenticated broadcast for severely resource-constrained environments. It achieves low energy consumption by keeping a consistent counter between sender and receiver, such that an initialization vector (IV) is not needed to be

appended to every packet. The main limitation of this platform was offered memory. In particular, the buffering restrictions limited the effective bandwidth of authenticated broadcast.

The existing ContikiSec [6] supports three security modes: confidentiality-only (ContikiSec-Enc), authentication-only (ContikiSec-Auth), and authentication with encipherment (ContikiSec-AE). ContikiSec offers the programmer the choice to select between three security levels depending on the needs of the application on hand. ContikiSec offers the programmer the choice to select between three security levels depending on the needs of the application on hand. In FlexiSec [7] is aimed to provide either message/entity authentication or a combination of confidentiality and authentication or that of confidentiality, authentication, and replay protection along with flexible selection of MAC sizes. The ContikiSec and FlexiSec mechanisms focus on secure network protocol and do not consider the data stored in nodes. In addition to secure network protocol the issue of access control in data storage receives considerable attention at all times. The MoteSec-Aware [8] provides the secure network protocol and access control. The secure network protocol is presented to detect the reply and jamming attacks. Access control method used to prevent unauthorized access. The MoteSec apply the symmetric key management for security, which suffers from a so-called orphan node problem.

The Secure and Efficient Data Transmission for CWSN [9] proposed two protocols SET-IBS and SET-IOOBS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. 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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

authentication. Thus, both SET-IBS and SET-IBOOS fully solve the orphan-node problem from using the symmetric key management for CWSNs. It achieves low energy consumption and minimum overhead. It is not suitable for resource limited sensor network. The Efficient online/Offline identity-based digital signature for WSN [10] could be effective for key management. It allows the offline information to be re-usable. Chaum's mixing approach [11] was shown to provide anonymous connections that protect against traffic analysis. Kong et al.[12] Proposed ANODR, an anonymous on demand routing for ad hoc networks.

3. SYSTEM MODEL

3.1 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 [13] [14], 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 data gathered by all sensor node of the cluster can be fused at the cluster-head, and only the gathered information needs to be communicated to the BS. 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. In CWSNs, data sensing, processing and transmission consume energy of sensor nodes. The cost of data transmission is much more expensive than that of data processing. Thus, the clustered architecture of WSNs that the CH node aggregates data and sends it to the BS is preferred, than the direct transmission of WSNs that a sensor node directly sends the data to the BS. A sensor node switches into sleep mode for energy saving when it does not involve in sensing or transmitting data, depending on the TDMA (time division multiple access) control used for data transmission.

3.2 Security Properties

3.2.1 Confidentiality: Confidentiality is a fundamental property of any secure communication system. Confidentiality guarantees that information is kept secret from unauthorized access. The typical way to achieve confidentiality is by using encryption.

3.2.2 Semantic Security: It guarantees that a adversary could not obtain partial information about the plaintext by observing the ciphertext.

3.2.3 Integrity: Integrity guarantees that the packet has not been modified during the transmission. It is achieved by including a digital signature, checksum and message integrity code (MIC).

3.2.4 Authenticity: Information authenticity guarantees that legitimate parties should be able to detect messages from unauthorized parties and drop them.

3.3 Attack Model

3.3.1 Active attack: Attackers can replay valid broadcast message of the previous transmission, for deceiving WSN nodes to carry out specified actions, such as providing adversaries with sensed data, or adjusting the node's local timer. Attackers can also modify or directly inject bogus broadcast messages to WSN, causing damage to the network.

3.3.2 Compromise attack: It is very common that WSN users are equipped with portable devices, this makes the WSN users vulnerable to compromise attack. For example, the attackers may physically capture the user's devices as well as the security information they store. Then attackers may use the compromised users to broadcast to the WSN. Furthermore, attackers may capture sensor nodes, obtain the secret they store, and then use the secret to undermine WSN.

3.3.3 Denial-of-Service (DoS) attack: (a) Attackers may flood bogus packets to WSN, causing WSN nodes to buffer all the messages received. Since the memory is very limited for sensor nodes, such local jamming attack will soon exhaust sensors' memory and block the subsequent broadcast messages. (b) Compared with the symmetric key operations, the public key operations require sensor nodes more battery power.

3.3.4 Replay attack: The attacker obtains the copy of a message in a sensor node and latter tries to reply it. This is carried out either by the sender or by an adversary who intercepts the data and retransmits it.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4 PROPOSED SYSTEM

In this paper, the IBCLA method is proposed. It uses IBS scheme [15] [16] [17] [18] [19] [20] to provide anonymity in WSNs. The proposed approach IBCLA is designed to protect cluster heads from attacker, because data aggregation and routing depend on the CHs fundamentally, attacks involving CHs could be the serious damaging to the network system. If the attacker knows the identity of aimed cluster heads means he easily capture that node and access all the information stored in that cluster heads. To overcome this problem the proposed IBCLA scheme provides the duplicate identity for the cluster heads by using Identity Based Digital Signature (IBS) used to prevent node capturing, compromised attack and authentication problem.

In this section, IBCLA is presented in detail. Before giving the detailed description, we first give an overview of IBS scheme.

4.1 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 public identity string, a sensor node generates a private key *sekID* associated with the ID using *msk*.

- *Signature Generation*: Given a message *M*, time-stamp *t* and a signing key *sekID* the sending node generates a signature *SIG*.

- *Verification*: Given the paramers *ID*, *M* and *SIG*, the receiving node outputs "accept" if *SIG* is valid, and outputs "reject" otherwise.

4.2 IBCLA Scheme for CWSNs

In IBCLA scheme implemented for CWSNs contains six operations. The four operations in the IBS scheme are also applicable in IBCLA additionally we have two operations that are transmitting digital signature (DS) as the cluster head's ID, and updating ID table. To calculate the current time and detection of reply attack we implement Virtual Counter Manager (VCM) in each CH. In MoteSec [4] they propose VCM for each sensor node that consumes more energy, here we implement VCM approach in cluster head nodes only, that reduces the energy as well as the buffering overhead.

- *Transmitting DS as the CH's ID*: *SIG* (M,t,β) here M indicate the message to be sent, t is the current time, β is the signing key, SIG is the digital signature. The signature is transmitted with the packet as the CH's id. While sending the packets from CH to BS, the messages are encrypted by using ID-based encryption (IBE).

- *Broadcasting CH's new ID*: During communication the CH broadcast the new ID in the network. The new ID is encrypted by using group key [21] [22]. Within the particular time period the CH's ID is again modified.

5 Id-Based Encryption

An identity-based encryption [23] scheme is specified by four steps: Setup, Extract, Encrypt, and Decrypt.

- *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.

- *Extract*: Given public identity string, a sensor node generates a private key *sekID* associated with the ID using *msk*.

- *Encrypt*: Takes as input *param*, ID and M. It returns a ciphertext C

- *Decrypt*: Takes as input param, ID, C and private key *sekID*. It returns M.

4.3 Virtual Counter Manager in CH

With the synchronized incremental counter, we construct a VCM within each cluster head node for initializing the counter and maintaining counter synchronization between the CH and BS. Several synchronization techniques proposed in [24] [25] [26] [27]. The synchronized incremental counter in CH increases one count per average delay automatically. The average delay is an experimental value, we define the maximum counter synchronization error (MCSE) to be an experiment based delay counter, δ, between CH and BS. In other words, when the packet transmission time is much longer than δ, the jamming attack can be detected at BS. If a packet does not suffer the jamming attack, the receiver applies a buffer filter to detect whether the packet suffers the replay attack.

4.3.1 Transmission of packet in CH: Assuming that the CH has started to send a packet to the BS. The CH gets a counter value used as an

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IV from VCM. The packets are transmitted in encrypted format using ID-based encryption scheme. Transmission of packets in CH using VCM is depicted in algorithm 1.

Algorithm 1: Transmission of packet in CH: VCM approach

Scenario: CH sends a message *msg* to node *BS*
Input: IV (from sender's VCM) and *sekID*
Output: the packet that processed via IBE

1) **if** *radio channel = success* **then**
2) Send out the packet ($CH\ new\ ID,\ BS\ ID,\ E_{BS\,ID}(msg)$);
3) **else**
4) Back off for a random period of time and then go To the step 1
5) **end if**

4.3.2 Reception of packet in BS: The BS will receive an incoming packet after propagation delay in the air. When receiving a packet successfully, the receiver node needs to perform two checks: (1) determine whether the packet is a legitimate one and (2) determine whether the packet has suffered attacks. The VCM at BS is depicted in algorithm 2.The BS gets a current counter value (CCV) from VCM and calculates a range counter interval (RCI)=[CCV − δ +1,CCV]. RCI is used as a set of IVs to verify the received packet. If all decryptions fail within the interval defined in RCI, then the packets may be jammed or invalid (e.g., severe fading). Under this circumstance, such packets are dropped. In order to detect replay attacks, we simply use a buffer to filter out duplicate packets. The receiver queries the corresponding buffer filter for the tuple (srcID, IV) of a packet. If the query returns "success," which means there actually does not have the duplicate tuples in the buffer filter, then the packet is considered to be a non-replayed packet and is consequently added into the buffer filter. Otherwise, the packet is treated as a replay and is consequently dropped.In IBCLA approach CH encrypts the data using the ID- based encryption scheme. The BS station obtain the original ID of CH from the ID table and use that as the public key to encrypt the received message of CH. The IBCLA uses IBS both authentication and identification. The messages are transmitted in encrypted format so data confidentiality achieved by IBCLA.

Algorithm 2: Reception of packet in BS: VCM approach

Scenario: BS receives a packet *M* from CH
Input: RCI (from BS's VCM)
Output: result of verification

1) **If** IBS.verify = TRUE **then**
2) Compute range counter interval (RCI)= $\{x/(CCV - \delta + 1) \le x \le CCV\}$;
3) Set index= 0;
4) **repeat**
5) **if** *IBE.decrypt(RCI[index]) ≠ success* **then**
6) index++;
7) **if** *index= δ* **then**
8) Drop the jammed packets out;
9) **end if**
10) **else**
11) **if** *check buffer-filter (SrIDr,RCI[index])=success* **then**
12) Store (SrcID,RCI[index]) into buffer filter;
13) **else**
14) Drop the replayed packets out;
15) **end if**
16) index= δ;
17) **end if**
18) **until** $index \neq \delta$;
19) **end if**

5 SIMULATION RESULTS AND ANALYSIS

5.1 Replay and Jamming Detection

To detect the replay and jamming δ being set to 3, we will classify large delays (> 3) as being the consequence of a jamming attack. Nevertheless, it is worth noting that the false negative probability is as low as 0.003, which can be obtained as 100%−99.7% = 0.3%, where the true delay is with 99.7% confidence. Next, the receiver uses the buffer filter to check each packet with a tuple (SrcID, IV) for detecting replay attack. If (SrcID, IV) is, in fact, an entry of the buffer filter, the buffer filter returns FALSE and drops the packet; otherwise, the tuple (SrcID, IV) is added to the buffer filter. Recall that the data structure of buffer filter is an array. Therefore, checking any single element in an array takes $O(1)$ time (average case).Moreover, the detection probability that can be achieved is 1.

Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5.2 Resilience Against Node Capture Attack

We consider the case where the adversary not only eavesdrops on the transmitted messages but trying to detect the identity of the node to capture the node. The IBCLA scheme provides the resilience against node capturing attack by introducing duplicate identity depends on actual identity. The IBCLA scheme achieves better throughput.

5.3 Resilience Against false data injection attack

Since attackers do not have valid digital signature to concatenate with broadcast messages for authentication, attackers cannot act as the CH to inject false data during communication. Therefore, IBCLA is resilient and robust to the sinkhole and selective forwarding attacks, because the BS is capable to ignore all the communication packets with bogus node IDs or bogus digital signatures. Together with IBS, the IBCLA resilient to the hello flood attacks involving CHs.

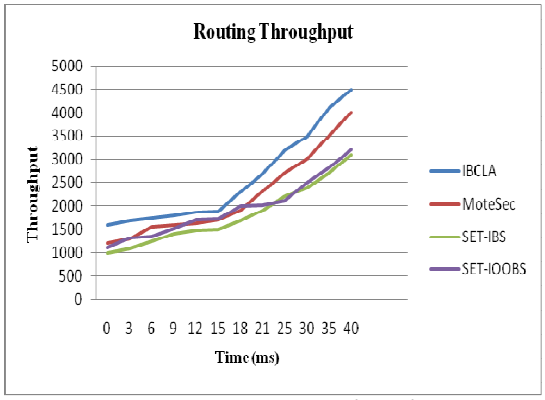

Fig. 1. Routing Throughput

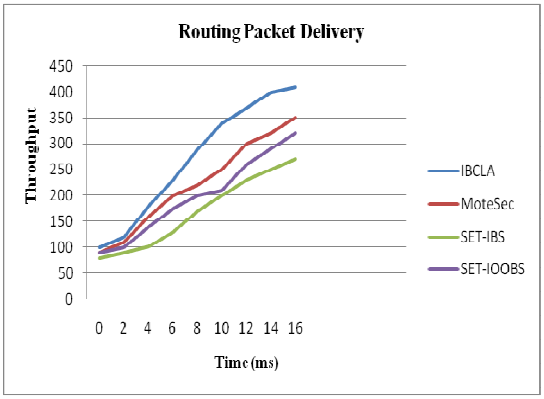

Fig. 2. Packet Delivery Ratio

In figure1 simulation result shows that the routing throughput is increased in proposed IBCLA method compared to MoteSec,SET-IBS and SET-IOOBS.

In figure2 simulation result shows packet delivery ratio is higher in our system than existing system. Thus the packet dropping and modification is minimized.

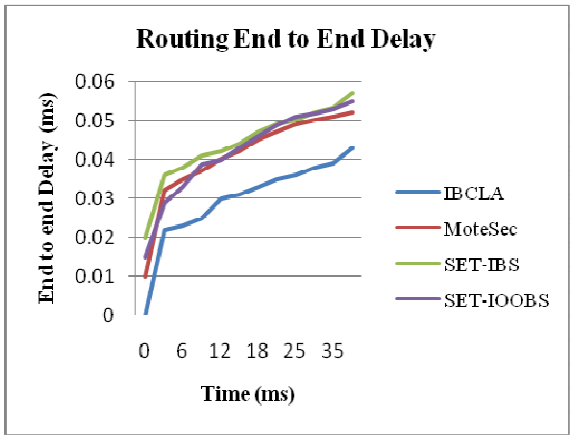

Fig. 3. Routing End To End Delay

In figure 3 simulation result shows that end to end delay is reduced in IBCLA compared to MoteSec, SET-IBS and SET-IOOBS

6. CONCLUSION

In this paper, we first reviewed the data communication issues and the security issues in CWSNs. The deficiency of the symmetric key management for clustered architecture of WSNs has been discussed. Then we presented IBCLA for CWSNs with VCM which achieve a detection of compromised node, node capturing, replay and jamming attacks .It also achieves anonymity in WSNs hence protect nodes identity from attackers. The IBCLA scheme simultaneously provides data secrecy, integrity and authenticity.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFRENCES:

[1] S. Misra and G. Xue, "Efficient anonymity schemes for clustered wireless sensor networks," *International Journal of Sensor Networks*,vol. 1, no. 1/2, pp. 50–63, 2006.

[2] W. Hu, P. Corke, W. C. Shih *et al.*, "SecFleck: A public key technology platform for wireless sensor networks," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer Verlag, 2009, pp. 296-311.

[3] W. Hu, H. Tan, P. Corke *et al.*, "Toward trusted wireless sensor networks," *ACM Trans. Sen. Netw.,* vol. 7, no. 1, pp. 1-25, 2010.

[4] J. J. Hwang, B. M. Shao, and P. C. Wang, "A new access control method using prime factorization," *The Computer*, vol. 35, no. 1, pp. 16–20, 1992.

[5] Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: security protocols for sensor networks," in *Proc. 2001 International Conference on Mobile Computing and Networking*, pp. 189–199.

[6] L. Casado and P. Tsigas, "Contikisec: a secure network layer for wirelesssensor networks under the Contiki operating system," in *Proc. 2009Nordic Conference on Secure IT Systems*, pp. 133–147.

[7] D. Jinwala, D. Patel, and K. Dasgupta, "FlexiSec: a configurable link layer security architecture for wireless sensor networks," *Inf. Assurance and Security*, vol. 4, no. 6, pp. 582–603, 2009.

[8] Yao-Tung Tsou, Chun-Shien Lu and Sy-Yen Kuo, "*M*oteSec-Aware: A Practical Secure Mechanism for Wireless Sensor Networks", *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2817–2829, June. 2013.

[9] Huang Lu, Jie Li and Mohsen Guizani, "Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks", *IEEE Trans. parallel and distributed system,*2013.

[10] J. Liu, J. Baek, J. Zhou *et al.*, "Efficient online/offline identity-based signature for wireless sensor network," *Int. J. Inf. Secur.*, vol. 9, no. 4, pp. 287–296, 2010.

[11] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp 84901981.

[12] J. Kong and X. Hong, "Anodr: anonymous on demand routing with untraceable routes for mobile ad-hoc networks." in *MobiHoc '03:Proceedings of the 4th ACM international symposium on Mobile adhoc networking & computing*, 2003, pp. 291–302.

[13] Bandyopadhyay, S. and Coyle, E. (2003) 'An energy efficient hierarchical clustering algorithm for wireless sensor networks', *22nd Conference of the IEEE Communication Society, INFOCOM*, Vol. 3.

[14] Younis, O. and Fahmy, S. (2004) 'Distributed clustering in adhoc sensor networks: a hybrid, energy-efficient approach',*23rd Conference of the IEEE Computer and Communications Societies*, pp.629–640.

[15] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Lect. Notes. Comput. Sc. - CRYPTO*, 1985, vol. 196, pp. 47–53.

[16] J. Sun, C. Zhang, Y. Zhang *et al.*, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227–1239, 2010.

[17] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," in *Lect. Notes. Comput. Sc. - CRYPTO*, 1990, vol. 435, pp.263–275.

[18] 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, vol. 4058, pp. 99–110.

[19] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature," in *Proc. IEEE GLOBECOM*, 2010, pp. 1–5.

[20] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures," in *Proc. IEEE CIT*, 2010, pp. 882–889.

[21] H. Harney and C. Muckenhirn, "Group key management protocol (gkmp) architecture," *IETF Request for Comments, RFC 2094*, 1997.C.

[22] 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, pp. 1–5.

[23] Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. In *Proceedings of Advances in Cryptology - CRYPTO '01*, volume 2139 of *LNCS*, pages 213–229. Springer, 2001.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[24] S. Ganeriwal, R. Kumar, and M. B. Srivastava, "Timing-sync protocol for sensor networks," in *Proc. 2003 International Conference on Networked Sensor Systems*, pp. 138–149.

[25] J. Elson, L. Girod, and D. Estrin, "Fine-grained network time synchronization using reference broadcasts," *ACM SIGOPS Operating Systems Review - Proc. 2002 Symposium on Operating Systems Design and Implementation*, vol. 36, no. SI, pp. 147–163.

[26] S. Ganeriwal, S. Capkun, and M. B. Srivastava, "Secure time synchronization in sensor networks," *ACM Trans. Inf. and Systems Security*, vol.11, no. 4, pp. 1–35, 2006.

[27] L. Shu, M. Hauswirth, Y. Zhang, J. Ma, G. Min, and Y. Wang, "Cross layer optimization for data gathering in wireless multimedia sensor networks within expected network lifetime," *J. Universal Computer Science*, vol. 16, no. 10, pp. 1343–1367, 2010.