INNOVATIVE SCIENCE AND TECHNOLOGY PUBLICATIONS

International Journal of Future Innovative Science and Technology
ISSN: 2454- 194X Volume - 2, Issue - 2

Manuscript Title

Energetic Wireless Sensor Networks Using Operative Key Managing With Certificate less Effective Key Management Protocol

[1]S. Thylashri, [2]C. Shanmuganathan, [3]Dr.P.Raviraj,

P.G. Scholar, Research Scholar, Prof.& HOD,
Dept. of Compuer Science and Engineering

[1]St.Peter's College of Engg.& Technology, Chennai, India
[2]Manonmaniam Sudaranar University, Tirunelveli,Tamilnadu, India
[3]Kalaigner Karunanidhi Inst.of Tech., Coimbatore,Tamilnadu,India

E-Mail: ***thylashri93@gmail.com, cshanme@yahoo.co.in,raviraj_it@yahoo.co.in***

May – 2016

www.istpublications.com

International Journal of Future Innovative Science and Technology, ISSN: 2454- 194X
Volume-2, Issue-2, May - 2016 editor@istpublications.com

Energetic Wireless Sensor Networks Using Operative Key Managing With Certificate less Effective Key Management Protocol

S. Thylashri,
P.G. Scholar. Dept. of CSE,
St.Peter's College of Engg.& Technology, Chennai, India
thylashri93@gmail.com

C. Shanmuganathan,
Research Scholar, Dept. of CSE,
Manonmaniam Sudaranar University,
Tirunelveli,Tamilnadu, India
cshanme@yahoo.co.in

Dr.P.Raviraj,
Prof.& HOD, Dept. of CSE
Kalaigner Karunanidhi Inst.of Tech.,
Coimbatore,Tamilnadu,India
raviraj_it@yahoo.co.in

ABSTRACT

Wireless sensing element networks have been deployed for a good kind of applications, including military sensing and trailing, patient standing observation, traffic flow observation, wherever sensory devices typically move between different locations. Securing knowledge and communications needs suitable coding key protocols. In this paper, we have a tendency to propose a certificate Less-effective key management (CL-EKM) protocol for secure communication in dynamic WSNs characterized by node mobility. The CL-EKM supports economical key updates once a node leaves or joins a cluster and ensures forward and backward key secrecy. The protocol additionally supports economical key revocation for compromised nodes and minimizes the impact of a node compromise on the protection of alternative communication links. A security analysis of our theme shows that our protocol is effective in defensive against numerous attacks. We implement CL-EKM in to WSN Network assess its time, energy, communication, and memory performance.

Keywords - Wireless sensor networks, Dynamic key management, Key revocation.

I. INTRODUCTION

DYNAMIC wireless sensor networks (WSNs), that modify quality of sensor nodes, encourage more extensive network coverage and more accurate service than static WSNs. Therefore, dynamic WSNs are being rapidly adopted in monitoring applications, such as target tracking in battlefield surveillance, healthcare frameworks, traffic flow and vehicle status monitoring [6]. In any case, sensor devices are exposed to malicious attacks such as impersonation, interception, and capture because of their slips of availability in wireless communication. Dynamic WSNs thus need to address key security necessities, like node authentication, data confidentiality and integrity, at whenever point and wherever the nodes move. All key management schemes should fulfill the subsequent ancient security requirements: confidentiality, authentication, originality, integrity and non-repudiation. A similar holds for dynamic key management schemes [6]. Additionally, consistent with the options and also the application environment of dynamic key management, some particular evaluation metrics are node revocation, forward and backward privacy, collusion conflict and key connectivity [1].

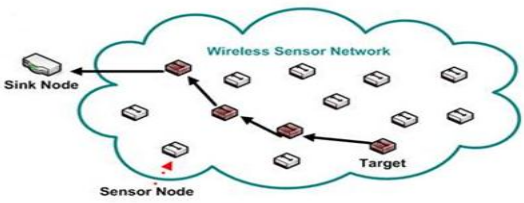

Fig. 1.Wireless Sensor Network.

In order to effectively give both node validation furthermore, set up a pairwise key between nodes, we fabricate CL-EKM by using a blending free certificateless hybrid signcryption plan (CL-HSC) proposed by us in a prior work [4], [2]. Because of the properties of CL-HSC, the pairwise key of CL-EKM can be competently shared between two nodes without requiring exhausting matching operations and the exchange of certificates. In this paper, we proposed a certificate less effective key management scheme which does not require online certification authority for secure communication. To sustain node mobility, our CL-EKM also maintain lightweight processes for cluster key upgrades performed when a node moves, and key revocation is implemented when a node is recognized as malicious or leaves the cluster permanently.CL-EKM is versatile if there should arise an occurrence of increments of new nodes after system arrangement. CL-EKM is secure against node compromise, cloning and impersonation, and guarantees forward and backward secrecy. The security efficiency of proposed scheme is portrayed in this paper.

II. RELATED WORKS

Symmetric key schemes aren't viable for mobile device nodes and therefore past approaches havetargeted solelyonstaticWSNs.Someapproaches are plan ned supported PKC to support dynamic WSNs. Thus, during this section, we have a tendency to review previous PKC-support key management method for dynamic WSNs and scrutinize their security weaknesses or disadvantages. Chuang et al. [11] and Agrawal et al. [7] planned a two-layered key management theme and a dynamic key update protocol in dynamic WSNs supported

the Diffie-Hellman (DH), severally. However, both schemes [11],[7] aren't fitted to sensors with restricted resources and unable to perform expensive computations with huge key sizes Since ECCis computationally more efficient and many approaches with certificate [6], [9],[12],[5] are planned supported ECC. Alagheband et al.[5] planned a key management theme by using ECC-based signcryption, but this theme is insecure against message forgery attacks [3]. However, we have a tendency to found the security weaknesses of their theme.

Du et al. [5] use a ECDSA theme to verify the identity of a cluster head and a static EC-Diffie-Hellman key agreement theme to share the pairwise key between the cluster heads. Therefore, the theme isn't secure against known-key attacks; On the other hand, Du et al. use a modular arithmetic-based symmetric key proceed to distribute the pairwise key between a sensor node and a cluster head. Thus, a sensor node cannot directly establish a pairwise key with alternative sensing element nodes and, instead, it needs the support of the cluster head. Then the cluster head transmits the encrypted pairwise key to every node. Therefore, their theme isn't compromise-resilient against cluster head capture, as a result of the cluster head at random generates a pairwise key between sensing element nodes whenever it's requested by the nodes. However, the theme doesn't give a method to protect against clone and impersonation attack.

III. OVERVIEW OF THE CERTIFICATE LESS EFFECTIVE KEY MANAGEMENT SCHEME

In this paper, we propose a Certificate less Key Management scheme (CL-EKM) that backing the foundation of four sorts of keys, to be specific: a corticated less public/private key pair, an individual key, a pairwise key, and a cluster key. This method also makes use of the main algorithms of the CL-HSC scheme [4] in deriving certificateless public/private keys and pairwise keys.

A. Certificate Less Public/Private Key

Prior to a node is conveyed, the KGC at the BS produces an one of a kind less private/public key pair and introduces the keys in the node. This key pair is utilized to create a commonly confirmed pairwise key

B. Individual Node Key

Every node imparts a remarkable individual key to BS. For instance, a sensor can utilize the individual key to encode a ready message sent to the BS. The BS can likewise utilize this key to encode any perceptive information.

C. Pairwise Key

Every node imparts an alternate pairwise key to each of its neighboring nodes for secure correspondences and confirmation of these nodes. In a collection steady WSN, the sensor can utilize its pairwise key to safely transmit the detected information to other sensor.

D. Cluster Key

All nodes in a cluster share a key, named as cluster key. The cluster key is essentially utilized for securing show messages as a part of a group, e.g. the change of part status in a cluster. Just the cluster head can redesign the group key when a sensor leaves or joins the cluster [7].

E. The Details of CL-EKM

The CL-EKM consists of 7 phases: system setup, pairwise key generation, cluster formation, key update, node movement, key revocation, and addition of a new node.

F. System Setup

Before the network deployment, the BS generates system parameters and registers the node by including it in a member list M.

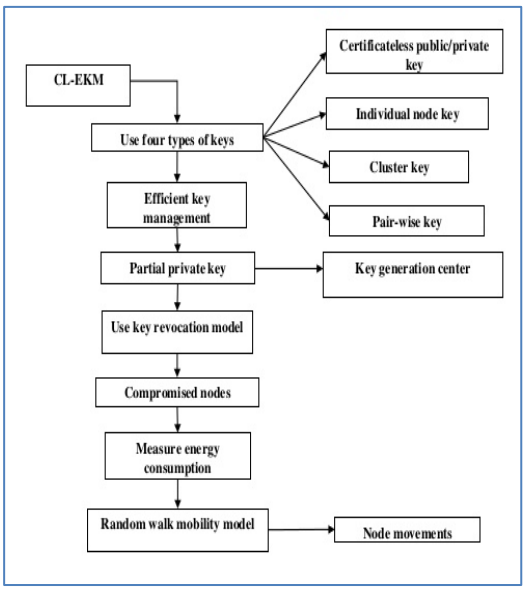

Fig. 2.Overview of CL-EKM

1) Generation of System Parameters

The KGC at the BS scamper the following steps by taking a security parameter k ∈ Zas the input, and returns a list of system parameter

- Choose a k-bit prime q
- Determine the tuple
- Choose the master private key and compute the system public key P
- Choose cryptographic hash functions

2) Node Registration

The BS assigns a novel identifier. Here we tend to describe the certificateless public/private key and individual node key operations. once the key generation for all the nodes, the BS generates a list M contains identifiers and public keys of all these nodes.

It conjointly initializes a revocation list R that list out the revoked nodes. The public/private key, and the individual key are installed within the memory of every node.

G. Pairwise Key Generation

After the network preparation, a node might broadcast an advertisement message to its neighborhood to activate the pairwise key setup with its neighbors. The advertisement messages have its identifier and public key.

At first, two nodes observed a long-term pairwise master key among them, which is then used to derive the pairwise encryption key. The pairwise encryption key is temporary and be able to utilize as a session key to encrypt detected information

1) Pairwise Master Key Establishment

In this section, we tend to describe the protocol for establishing a pairwise master key between any two nodes nA and nB with distinctive IDs A and B, severally.

2) Pairwise Encryption Key Establishment

Some time nA and nB set the pairwise master key KAB, they generate an HMAC of KAB. The HMAC is then valid by each nA and nB. If the validation is thriving, the HMAC value is established because the short-term pairwise encryption key kAB.

H. Cluster Formation

Once the nodes area unit deployed, each sensor discovers neighboring sensors through beacon message exchanges and then payoff to manifest them. If the authentication is successful, forms a cluster with the authenticated sensors and that they share a standard cluster key.

1) Node Discovery and Authentication

For node discovery, broadcasts an advertisement message. Note that it receives multiple advertising messages if it's among the range of over one sensor.

However, it must choose one sensor, is also by prioritizing over the proximity and signal strength. once it selects multiple cluster heads and sends a response to to any or all of them, it is considered as a compromised node.

2) Cluster Key Generation

If it fails to visualize, discards the message and reports to the BS as an illegitimate cluster head. Otherwise, it test the validity. If the validity test fails, discards the message.

3) Membership Validation

After discovering all the neighboring nodes, the BS checks the validity of the nodes. If all nodes area unit legitimate, the BS sends an acknowledgement. Otherwise, the BS rejects and investigates the identities of invalid nodes.

I. Key Update

In order to safeguard against cryptanalysis and diminish harm from compromised keys, regular encryption key updates unremarkably needed. During this section we tend to provide the pairwise key update and cluster key update operations.

1) Pairwise Key Update

To revise a pairwise encryption key, two nodes that shared the pairwise key perform a Pairwise Encryption Key Establishment process. On the opposite hand, the pairwise master key doesn't need periodical updates. As long because the nodes don't seem to be compromised, the pairwise master keys cannot be exposed. However, if a pairwise master key is modified or must to be updated, the Pairwise Master Key Establishment method should be executed.

2) Cluster Key Update

Only cluster head sensors will update their cluster key. If a sensor tries to alter the cluster key, the node is taken into account a malicious node.

J. Node Movement

When a node moves between clusters, the sensors must properly manage the cluster keys to confirm the forward/backward secrecy. Thus, the sensor updates the cluster key and notifies the BS of the modified node status.

1) Node Leave

A node could leave a cluster due to node failure, location amendment or intermittent communication failure. There area unit each proactive and reactive ways that for cluster head to notice once a node leaves the cluster. The proactive case occurs when the node actively decides to leave the cluster and notifies the cluster head or the cluster head decides to revoke the node. The reactive case happens once the cluster head fails to communicate .It may happen that a node expire out of battery power, fall short to connect due to interference or obstacles, is captured by the assaulter or is touched accidentally. Since the nodes in a very cluster sporadically exchange light-weight beacon messages, once it doesn't receive the beacon message for a predetermined time period & notice as disappeared node.

2) Node Join

Once the moving node leaves a cluster, it should be a part of different clusters or return to the previous cluster after some period.

a) Join a New Cluster:

Sends a join request to hitch a cluster. when receives the join request, perform Pairwise Key Generation procedure to the BS. The BS decrypts the message and validates whether it could be a legitimate node or not and sends an acknowledgement. In case of node validation failure at the BS stops this process and revokes the pairwise key .Once receives the acknowledgement, it performs the Cluster Key Update method with all different nodes within the cluster.

b) Return to the Previous Cluster

Perform solely the Pairwise Encryption Key Establishment procedure to form a replacement pairwise encryption key. Then, the cluster head additionally updates the cluster key to safeguard backward key secrecy. Once the BS decrypts the message and determines that nis a legitimate node, the BS launch the acknowledgement. Once accept the acknowledgement, it performs the Cluster Key Update method with all different nodes within the cluster.

K. Key Revocation

We assume that the BS will find compromised sensors the BS will utilize the updated node status information of every cluster to analyze an abnormal node. In our protocol, a cluster head reports the amendment of its node status to the BS, like whenever a node joins or leaves a cluster. For example, the BS will take into account a node as compromised if the node disappears for a certain period of

time. During this procedure, we offer a key revocation method to be used once the BS discovers a compromised node or a compromised cluster head.

1) Compromised Node

The BS creates a CompNode message and it sends to all .After all sensors decrypt the message, the connected keys are discarded. different than performs the Node leave operations to vary this cluster key with the enduring constituent nodes.

2) Compromised Cluster Head

when the BS generates a CompHeader message and it sends the message to any or all. Once all nodes decrypt the message, they discard the related keys. Then, each attempts to find different neighboring cluster heads and performs the Join different cluster steps of the Node join method with the neighboring cluster head. If some Node is unable to find a different cluster head node, it should apprize the BS by perform the Join different cluster steps

L. Addition of a New Node

Before adding a replacement node into Associate existing network, the BS should make sure that the node isn't cooperate. The new node establishes a full private/public key through the node registration part in line with the distance and also the strength of signal, it initiates the Pairwise Key Generation procedure. so as to produce backward secrecy, performs Cluster Key Update procedure

IV. EXPERIMENTAL RESULT

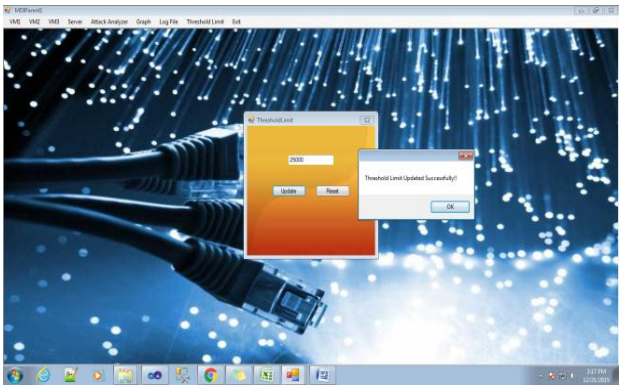

Fig. 3.Updating threshold limit

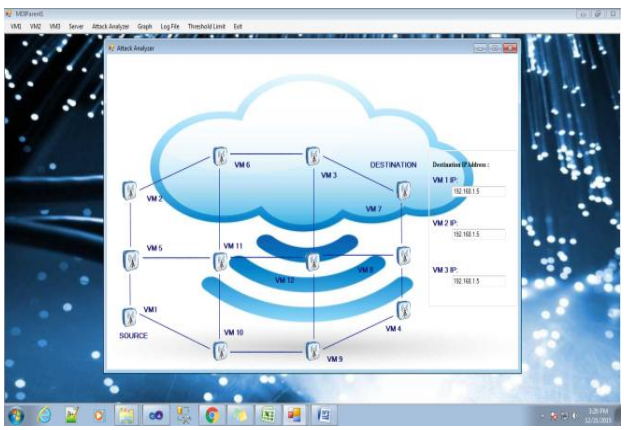

Fig. 4.Assigning source and destination nodes

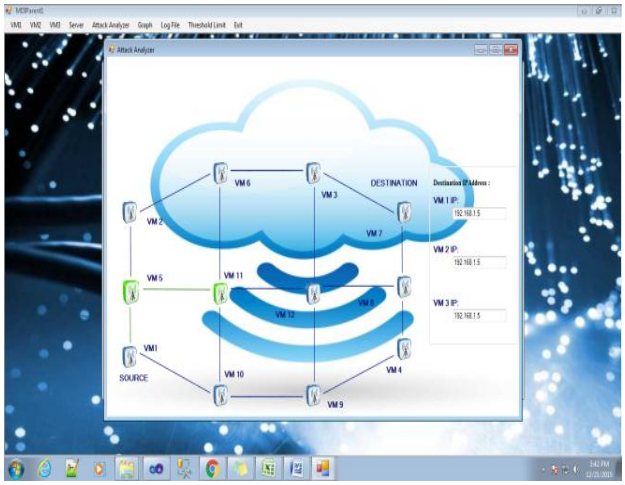

Fig. 5.Sending data to destination

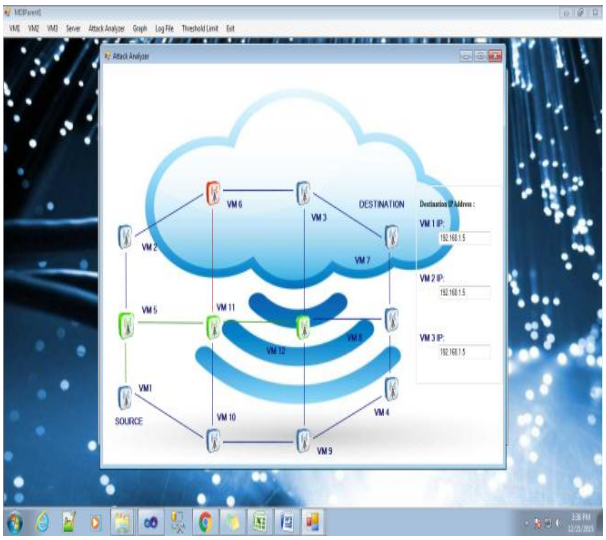

Fig. 6.Identifying malicious node

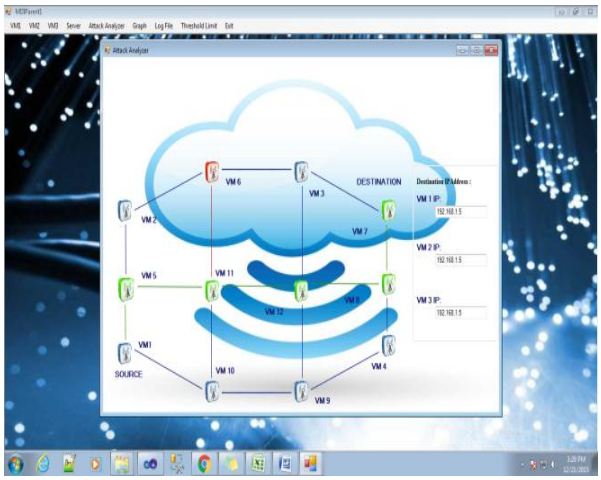

Fig. 7.Data sends to destination

V. PERFORMANCE EVALUATIONS

In this section, we estimate and compare the performance of the CL-EKM protocol along with the CL-

HSC protocol. Simulation results show that our proposed scheme satisfies all security requirements and withstand all node attacks.

Fig. 8 shows the result after performance evaluation. The x-axis gives the number of compromised nodes and the y-axis indicates the delay occurred in the protocol. The diagram gives the reasonable shot of the delay taken by the protocols relying upon their compromised nodes.

The next graph i.e. Fig. 9, the correlation between key Generations got to against the time or the time taken for processing these Keys. The graph clearly indicates how the CL-EKM protocol is ended up being quicker when contrasted with that of the CL-HSC protocol

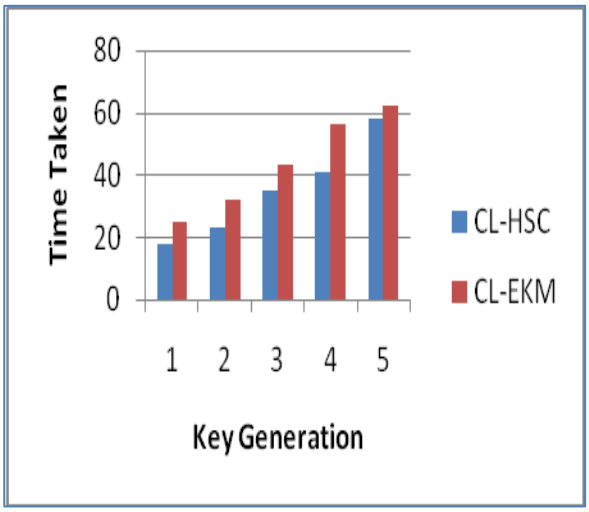

Fig. 8.Analysis graph for delay in various compromised nodes

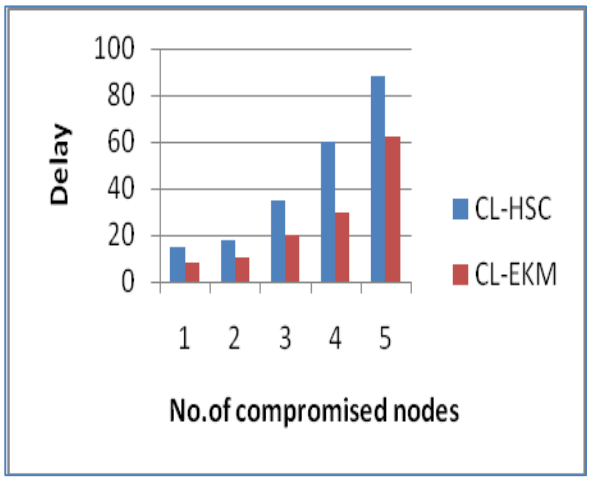

Fig. 9.Analysis graph of Time Consumption for key Generation

VI. CONCLUSION

In this paper, we tend to propose the certificate less effective key management protocol (CL-EKM) for secure communication in dynamic WSNs. CL-EKM sustain efficient communication for key updates and management once a node leaves or joins a cluster and thus ensures forward and backward key secrecy. Our theme is resilient against node compromise, cloning and impersonation attacks and protects the information confidentiality and integrity. The experimental results demonstrate the efficiency of CL-EKM in resource strained WSNs.

REFERENCES

[1] Seung-Hyun Seo, Salmin Sultana, "Effective Key Management in Dynamic Wireless Sensor Networks," IEEE Transactions On Information Forensics And Security, Vol. 10, No. 2, February 2015.

[2] S. H. Seo, J. Won, and E. Bertino, "POSTER: A pairing-free certificateless hybrid signcryption scheme for advanced metering infrastructures,"in*Proc. 4th ACM CODASPY*, 2014, pp. 143–146.

[3] X.-J. Lin and L. Sun, "Cryptanalysis and improvement of a dynamic and secure key management model for hierarchical heterogeneous sensor networks," in *Proc. IACR Cryptol. ePrint Archive*, 2013, pp. 698–698.

[4] S. Seo and E. Bertino, "Elliptic curve cryptography based certificateless hybrid signcryption scheme without pairing," CERIAS, West Lafayette, IN, USA, Tech. Rep. CERIAS TR 2013-10, 2013. [Online]. Available: https://www.cerias.purdue.edu/apps/reports_and_papers/.Seung-Hyun.

[5] D. Du, H. Xiong, and H. Wang, "An efficient key management scheme for wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 2012,Sep. 2012, Art. ID 406254.

[6] M. R. Alagheband and M. R. Aref, "Dynamic and secure key management model for hierarchical heterogeneous sensor networks," *IET Inf.Secur.*, vol. 6, no. 4, pp. 271–280, Dec. 2012.

[7] S. Agrawal, R. Roman, M. L. Das, A. Mathuria, and J. Lopez, "A novel key update protocol in mobile sensor networks," in *Proc. 8th Int. Conf.ICISS*, vol. 7671. 2012,pp. 194–207.

[8] X. Zhang, J. He, and Q. Wei, "EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks," *EURASIPJ. Wireless Commun. Netw.*, vol. 2011, pp. 1–11, Jan. 2011.

[9] I.-H. Chuang, W.-T. Su, C.-Y. Wu, J.-P. Hsu, and Y.-H. Kuo, "Two layered dynamic key management in mobile and long-lived cluster based wireless sensor networks," in *Proc. IEEE WCNC*, Mar. 2007, pp. 4145–4150.

[10] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fast authenticated key establishment protocols for self-organizing sensor networks," in *Proc. 2nd ACM Int. Conf. WSNA, 2003 ,pp.141-15.*