# Effective key management in Dynamic WSN

K.Nartkannai, Dr H Shaheen

*Assistant Professor,Department of CSE, St.Peter's Engineering College,Hyderabad*
*Associate Professor,Department of CSE, St.Peter's Engineering College,Hyderabad*

***Abstract***

*Recently, wireless sensor networks (WSNs) have been deployed for a wide variety of applications, including military sensing and tracking, patient status monitoring, traffic flow monitoring, where sensory devices often move between different locations. Securing data and communications requires suitable encryption key protocols. In this paper, we propose a certificateless-effective key management (CL-EKM) protocol for secure communication in dynamic WSNs characterized by node mobility. The CL-EKM supports efficient key updates when a node leaves or joins a cluster and ensures forward and backward key secrecy. The protocol also supports efficient key revocation for compromised nodes and minimizes the impact of a node compromise on the security of other communication links. A security analysis of our scheme shows that our protocol is effective in defending against various attacks.We implement CL-EKM in Contiki OS and simulate it using Cooja simulator to assess its time, energy, communication, and memory performance.*

***Index Terms***—*Wireless sensor networks, certificateless public key cryptography, key management scheme.*

## I. INTRODUCTION

Dynamic wireless sensor networks (WSNs), which enable mobility of sensor nodes, facilitate wider 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 systems, traffic flow and vehicle status monitoring, dairy cattle health monitoring. However, sensor devices are vulnerable to malicious attacks such as impersonation, interception, capture or physical destruction, due to their unattended operative environments and lapses of connectivity in wireless communication. Thus, security is one of the most important issues in many critical dynamic WSN applications. Dynamic WSNs thus need to address key security requirements, such as node authentication, data confidentiality and integrity, whenever and wherever the nodes move. To address security, encryption key management protocols for dynamic WSNs have been proposed in the past based on symmetric key encryption. Such type of encryption is well-suited for sensor nodes because of their limited energy and processing capability. However, it suffers from high communication overhead and requires large memory space to store shared pair wise keys. It is also not scalable and not resilient against compromises, and unable to support node mobility. Therefore symmetric key encryption is not suitable for dynamic WSNs. More recently, asymmetric key based approaches have been proposed for dynamic WSNs.In this paper, we present a certificateless effective key management (CL-EKM) scheme for dynamic WSNs. In certificateless public key cryptography (CL-PKC) [12], the user's full private key is a combination of a partial private key generated by a key generation center (KGC) and the

ISSN: 2005-4262 IJGDC

user's own secret value. The special organization of the full private/public key pair removes the need for certificates and also resolves the key escrow problem by removing the responsibility for the user's full private key. We also take the benefit of ECC keys defined on an additive group with a 160-bit length as secure as the RSA keys with 1024-bit length.

## II. LITERATURE SURVEY

### *1. Compressive Sensing Over Networks*

In this system, we demonstrate some applications of compressive sensing over networks. We make a connection between compressive sensing and traditional information theoretic techniques in source coding and channel coding. Our results provide an explicit trade-off between the rate and the decoding complexity. The key difference of compressive sensing and traditional information theoretic approaches is at their decoding side. Although optimal decoders to recover the original signal, compressed by source coding have high complexity, the compressive sensing decoder is a linear or convex optimization. First, we investigate applications of compressive sensing on distributed compression of correlated sources. Here, by using compressive sensing, we propose a compression scheme for a family of correlated sources with a modularized decoder, providing a trade-off between the compression rate and the decoding complexity. We call this scheme *Sparse Distributed Compression*. We use this compression scheme for a general multicast network with correlated sources. Here, we first decode some of the sources by a network decoding technique and then, we use a compressive sensing decoder to obtain the whole sources. Then, we investigate applications of compressive sensing on channel coding. We propose a coding scheme that combines compressive sensing and random channel coding for a high-SNR point-to-point Gaussian channel. We call this scheme *Sparse Channel Coding*. We propose a modularized decoder providing a trade-off between the capacity loss and the decoding complexity. At the receiver side, first, we use a compressive sensing decoder on a noisy signal to obtain a noisy estimate of the original signal and then, we apply a traditional channel coding decoder to find the original signal.

### *2. Compressive Data Gathering for Large-Scale Wireless Sensor Networks*

This system presents the first complete design to apply compressive sampling theory to sensor data gathering for large scale wireless sensor networks. The successful scheme developed in this research is expected to offer fresh frame of mind for research in both compressive sampling applications and large-scale wireless sensor networks. We consider the scenario in which a large number of sensor nodes are densely deployed and sensor readings are spatially correlated. The proposed compressive data gathering is able to reduce global scale communication cost without introducing intensive computation or complicated transmission control. The load balancing characteristic is capable of extending the lifetime of the entire sensor network as well as individual sensors. Furthermore, the proposed scheme can cope with abnormal sensor readings gracefully. We also carry out the analysis of the network capacity of the proposed compressive data gathering and validate the analysis through ns-2 simulations. More importantly, this novel compressive data gathering has been tested on real sensor data and the results show the efficiency and robustness of the proposed scheme.

### *3. Compressive Data Gathering Scheme for Wireless Sensor network-a review*

In this system, we present a brief review of compressive sensing (CS) applied to the wireless sensor web. In wireless sensor networks (WSNs) the sampling rate of the sensors determines the pace of its energy use since most of the energy is used in sampling and transmission. To economize the energy in WSNs and thus extend the network lifetime, CS theory used to downplay the number of samples taken by sensor nodes. And also CS finds its applications in information gathering for large wireless sensor networks (WSNs), consisting of thousands of sensors deployed for tasks like infrastructure or environmental monitoring. This advance of using compressive data gathering (CDG) helps in overcoming the challenges of high communication costs.

### *4. Random Access Compressed Sensing in Underwater Sensor Networks*

In this system, we propose a power-efficient underwater sensor network scheme employing compressed sensing and random channel access. The proposed scheme is suitable for applications where a large number of sensor nodes are deployed uniformly over a certain area to measure a physical phenomenon. The underlying assumption is that most physical phenomena have sparse representations in the frequency domain. The network is assumed to have a Fusion Center (FC) that collects the observations of sensor nodes and reconstructs the measured field based on the obtained measurements. The proposed method is completely decentralized, i.e., sensor nodes act independently without the need for coordination with each other or with the FC. During each frame, a Bernoulli random generator at each node determines whether the node participates in sampling or stays inactive during that sampling period. If selected, it measures the physical quantity of interest, e.g. temperature. A second random generator with a uniform distribution then picks a (random) delay for the node to send its data to the FC. The proposed network scheme, referred to as Random Access Compressed Sensing (RACS), results in a simple power-efficient design, for: a) it eliminates the need for duplexing, which requires coordination from the FC; b) there is no need for acknowledgment packets and retransmissions in case packets collide; and moreover, c) it is efficient in terms of the communication resources used (only a small fraction of nodes sample and transmit in each sampling period).

### *5. Signal Recovery from Random Measurements via Orthogonal Matching Pursuit*

This system demonstrates theoretically and empirically that a greedy algorithm called Orthogonal Matching Pursuit (OMP) can reliably recover a signal with m nonzero entries in dimension d given O (mln d) random linear measurements of that signal. This is a massive improvement over previous results, which require O (m2) measurements. The new results for OMP are comparable with recent results for another approach called Basis Pursuit (BP). In some settings, the OMP algorithm is faster and easier to implement, so it is an attractive alternative to BP for signal recovery problems.

## III. PROPOSED SYSTEM

In this paper, we present a certificateless effective key management (CL-EKM) scheme for dynamic WSNs.

In certificateless public key cryptography (CL-PKC), the user’s full private key is a combination of a partial private key generated by a key generation center (KGC) and the user’s own secret value.

The special organization of the full private/public key pair removes the need for certificates and also resolves the key escrow problem by removing the responsibility for the user's full private key.

We also take the benefit of ECC keys defined on an additive group with a 160-bit length as secure as the RSA keys with 1024-bit length.

### Advantages of Proposed System

- 1.Provide more security
- 2.Decrease the overhead
- 3.Protects the data confidentiality and integrity

## IV.RESULT PORTRAITURE

- **Service provider:**

In this module, the service provider will browse the data file and then send to the particular receivers. Service provider will send their data file to router and router will connect to clusters, in a cluster highest energy sensor node will be activated and send to particular receiver (A, B, C…). And if any attacker will change the energy of the particular sensor node, then service provider will reassign the energy for sensor node.

- **Router**

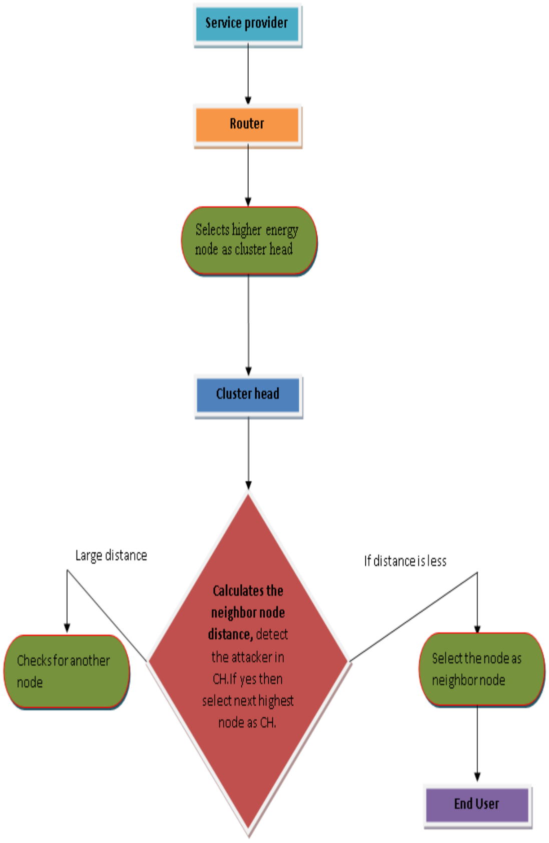
The Router manages a multiple clusters (cluster1, cluster2, cluster3, and cluster4) to provide data storage service. In cluster n-number of nodes (n1, n2, n3, n4…) are present, and in a cluster the sensor node which have more energy considered as a cluster head and it will communicate first. In a router service provider can view the node details, view routing path, view time delay and view attackers. Router will accept the file from the service provider, the cluster head will select first and it size will reduced according to the file size, then next time when we send the file, the other node will be cluster head. Similarly, the cluster head will select different node based on highest energy. The time delay will be calculated based on the routing delay. Attacker will be found if malicious data is added to corresponding node.

- **Cluster**

In cluster n-number nodes are present and the clusters are communicates with every clusters (cluster1, cluster2, cluster3 and cluster4).In a cluster the sensor node which have more energy considered as a cluster head. The service provider will assign the energy for each & every node. The service provider will upload the data file to the router; in a router clusters are activated and the cluster-based networks, to select the highest energy sensor nodes, and send to particular receivers.

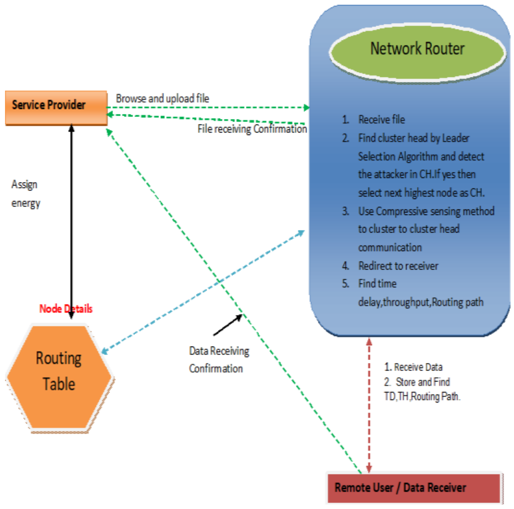
- **Receiver (End User )**

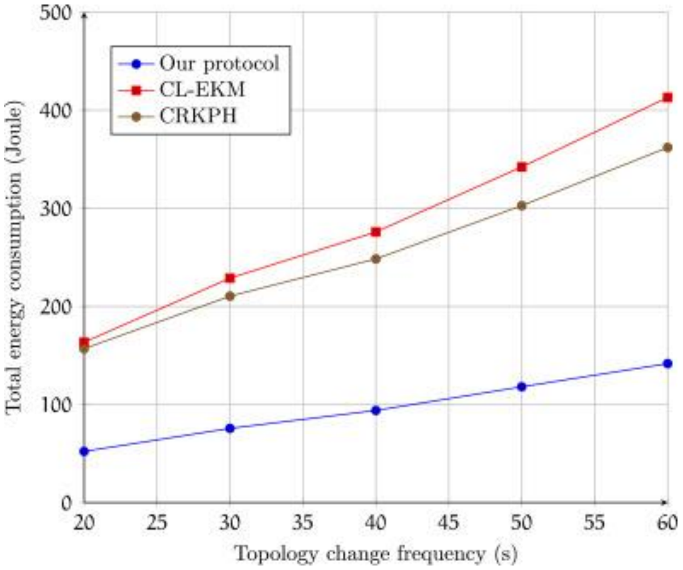
In this module, the receiver can receive the data file from the service provider via router. The receivers receive the file by without changing the File Contents. Users may receive particular data files within the network only.


Service provider
Router
Selects higher energy node as cluster head
Cluster head
Large distance
If distance is less
Calculates the neighbor node distance, detect the attacker in CH.If yes then select next highest node as CH.
Checks for another node
Select the node as neighbor node
End User

- **Attacker**

Attacker is one who is injecting the fake energy to the corresponding sensor nodes. The attacker decries the energy to the particular sensor node. After attacking the nodes, energy will be changed in a router.

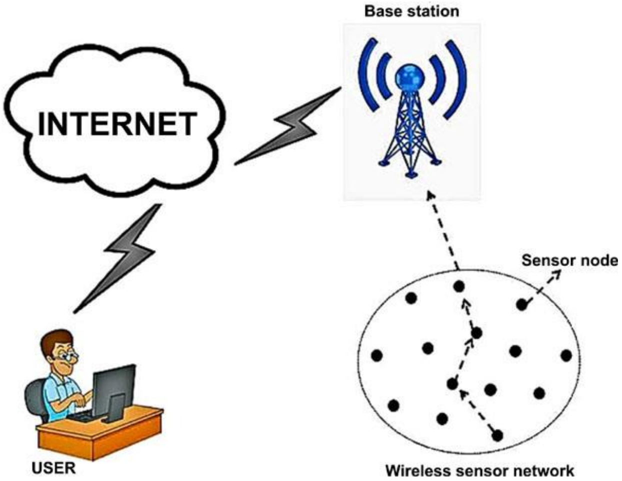

Network Router
Service Provider
Browse and upload file
File receiving Confirmation
1. Receive file
2. Find cluster head by Leader Selection Algorithm and detect the attacker in CH.If yes then select next highest node as CH.
3. Use Compressive sensing method to cluster to cluster head communication
4. Redirect to receiver
5. Find time delay,throughput,Routing path
Assign energy
Node Details
Routing Table
Data Receiving Confirmation
1. Receive Data
2. Store and Find TD,TH,Routing Path.
Remote User / Data Receiver



## IMPLEMENTATION

The Output from the computer is required to mainly create an efficient method of communication within the company primarily among the project leader and his team members, in other words, the administrator and the clients. The output of VPN is the system which allows the project leader to manage his clients in terms of creating new clients and assigning new projects to them, maintaining a record of the project validity and providing folder level access to each client on the user side depending on the projects allotted to him. After completion of a project, a new project may be assigned to the client. User authentication procedures are maintained at the initial stages itself. A new user may be created by the administrator himself or a user can himself register as a new user but the task of assigning projects and validating a new user rests with the administrator only.

The application starts running when it is executed for the first time. The server has to be started and then the internet explorer in used as the browser. The project will run on the local area network so the server machine will serve as the administrator while the other connected systems can act as the clients. The developed system is highly user friendly and can be easily understood by anyone using it even for the first time.



## V. CONCLUSION

ISSN: 2005-4262 IJGDC

In this paper, we propose the first certificateless effective key management protocol (CL-EKM) for secure communication in dynamic WSNs. CL-EKM supports efficient communication for key updates and management when a node leaves or joins a cluster and hence ensures forward and backward key secrecy. Our scheme is resilient against node compromise, cloning and impersonation attacks and protects the data confidentiality and integrity. The experimental results demonstrate the efficiency of CL-EKM in resource constrained WSNs. As future work, we plan to formulate a mathematical model for energy consumption, based on CL-EKM with various parameters related to node movements. This mathematical model will be utilized to estimate the proper value for the *Thold*and *Tbackoff* parameters based on the velocity and the desired tradeoff between the energy consumption and the security level.

## References

[1] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in *Proc. IEEE Symp. SP*, May 2003, pp. 197–213.

[2] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, “A key predistribution scheme for sensor networks using deployment knowledge,” *IEEE Trans.Dependable Secure Comput.*, vol. 3, no. 1, pp. 62–77, Jan./Mar. 2006.

[3] W. Du, J. Deng, Y. S. Han, P. Varshney, J. Katz, and A. Khalili, “A pairwise key predistribution scheme for wireless sensor networks,” *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 2, pp. 228–258, 2005.

[4] M. Rahman and K. El-Khatib, “Private key agreement and secure communication for heterogeneous sensor networks,” *J. Parallel Distrib.Comput.*, vol. 70, no. 8, pp. 858–870, 2010.

[5] 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.

[6] D. S. Sanchez and H. Baldus, “A deterministic pairwise key predistribution scheme for mobile sensor networks,” in *Proc. 1st Int. Conf.SecureComm*, Sep. 2005, pp. 277–288.

[7] I.-H. Chuang, W.-T. Su, C.-Y. Wu, J.-P. Hsu, and Y.-H. Kuo, “Twolayered dynamic key management in mobile and long-lived clusterbased wireless sensor networks,” in *Proc. IEEE WCNC*, Mar. 2007, pp. 4145–4150.

[8] 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.

[9] S. U. Khan, C. Pastrone, L. Lavagno, and M. A. Spirito, “An energy and memory-efficient key management scheme for mobile heterogeneous sensor networks,” in *Proc. 6th Int. Conf. CRiSIS*, Sep. 2011, pp. 1–8.

ISSN: 2005-4262 IJGDC

[10] 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.

[11] Dr.H. Shaheen, “Secured Message Exchange in Mission Critical Infrastructure using Conditional Privacy Preserving Authentication”, “International Journal of Computer and Mathematical Science”, Volume 7, Issue 5, May 2018, ISSN 2347-8527.