Abstract: Now days, Wireless sensor networks (WSNs) are widely used in wide variety of application so to improve security for WSNs and to protect the WSNs from various attack uses key management which is an effective way. A suitable encryption key protocol are used to secure data and communication. In this paper, a certificate less – effective key management (CL-EKM) protocol is proposed to have secure communication in dynamic WSNs characterized by node mobility. The CL-EKM protocol supports an economical communication for key updates and manages once a node joins or leaves a cluster and ensures forward and backward key secrecy. A protocol also supports key revocation for compromised nodes and to minimize the impact of a node compromise on the protection of alternative communication links. The security analysis states that CL-EKM protocol is effective in defensive against varied attacks.

Keywords: Wireless sensor networks, Certificate less public key cryptography, Key management schema.
Xu Li, Rongxing Lu, Xiaohui Liang, and Xuemmin (Sherman) Shen,[2] describe the novel key agreement protocol which is based on pairing-based cryptography over an elliptic curve. With the help of this protocol, if any two nodes want to communicate independently can use the same secret key by using pairing and identity-based encryption properties. The proposed technique reduces the key space of a node and also shows that it is robust against various attacks such as masquerade attacks, reply attacks, and message manipulation attacks.

X. Zhang, J. He, and Q. Wei[3] describe the energy-efficient distributed deterministic key management scheme (EDDK). With the help of this scheme pairwise keys and cluster keys of sensor nodes are well established as well as maintained securely and communication overhead is also less. They also made use of elliptic curve digital signature algorithm in EDDK, which provided the support for the establishment of pairwise keys and local cluster keys under the node mobility scenario.

N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz[4] describe the light-weighted implementation of public key called as cluster based public infrastructure (CBPKI), it is based on security and the authenticity of base station for executing a set of handshakes that establish session keys between the base station and sensors over the networks that are used for ensuring the data confidentiality and integrity.

III. System Model

3.1 Network Model

The scheme is meant for protecting WSN from malicious attacks. The network is secured using the proposed scheme which takes care of initialization, secure key distribution, key update and key revocation.

3.2 Overview of the proposed scheme

We implemented attack analyzer which takes care of security issues besides ensuring that the communications in the network are protected from malicious attacks. The controller sensor nodes and the attack analyzer work in tandem with each other in order to prevent attacks and promote secure communications. The users full private key's combination of a partial non-public key generating by a Key Generation Center (KGC) and therefore the user's secret price. Special Organization of the complete private/public key combine removes the requirement for the certificate. Effective sharing between 2 nodes while not requiring onerous pairing operations and therefore the exchange of certificate. We present a certificate-less effective key management (CL-EKM) scheme for dynamic WSNs. With the development of science and technology, cryptography has also been considerable development both in theory and in practice. For different applications, there are many different cryptography systems, such as the symmetric cryptography, public key cryptography and so on. All of these algorithms have the strengths and weaknesses in different applications, but we have not found that a theory which would be able to meet all application requirements in the WSNs. The most common WSN architecture follows the OSI architecture Model. The architecture of the WSN includes five layers and three cross layers. Mostly in sensor n/w, we require five layers, namely application, transport, n/w, data link & physical layer. The three cross planes are namely power management, mobility management, and task
management. These layers of the WSN are used to accomplish the n/w and make the sensors work together to raise the complete efficiency of the network. Please follow the below link for Types of wireless sensor networks and WSN topologies.

**IV. System Architecture**

[WSN System Architecture]

**Cl-Ekm Architecture**

**V. Conclusion And Future Enhancement**

We have a tendency to given an outline of state of the art dynamic key management schemes in WSNs. With the wide application of WSNs, in concert of the basic security problems, dynamic key management is attracting additional attention from the researchers and industrial engineers and lots of schemes were already planned. we have a tendency to mentioned the fundamental necessities of dynamic key management in WSNs, surveyed the planned themes for these environments and highlighted the safety and Performance benefits and downsides of every scheme. Finally, we've got summarized and analyzed these techniques in line with the mentioned analysis metrics.

**Acknowledgment**

My heartfelt gratitude goes to my beloved guide Mrs.S.Jayabharathi Assistant Professor, Department of Computer Science, Vivekanandha College for Women, Tiruchengode, India for dedication and patience in assigning me her valuable advice and efforts during the course of my studies.

**References**


