Key Management Schemes In Wireless Sensor Network: A Survey

[1]Nihar Ranjan Sabat [2] Sudhir Kumar Senapati
Faculty MCA Department
College Of It And Management Education, Bhubaneswar, India
[1]n.ranjan9@gmail.com [2]sudhir.aricent@gmail.com

Abstract:- **Key management is the provisions made in a cryptography system design that are related to generation, exchange, storage, safeguarding, use, vetting, and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols. Key management concerns keys at the user level, either between users or systems. Successful key management is critical to the security of a cryptosystem. In practice it is arguably the most difficult aspect of cryptography because it involves system policy, user training, organizational and depart mental interactions, and coordination between all of these elements. These concerns are not limited to cryptographic engineering. Key management requires both technical and organizational decisions, and as a result, some aspects of key management risk being neglected by managers and engineers, out of concern that the problem is technical or managerial, respectively. As wireless sensor networks continue to grow, so does the need for effective Security mechanisms. Because sensor networks may interact with sensitive data and operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the system design .However, due to inherent resource and computing constraints , security in sensor networks posses different challenges than traditional network or computer security. There is currently enormous research potential in the field of wireless sensor network security. Key has an important role in cryptographic security issues.. This paper presents a survey on various existing key management schemes for wireless sensor networks.**

Keywords- **Security, Design, Sensor networks, Key management, Key pre distributions**

I.INTRODUCTION

Wireless sensor networks consist of spatially distributed sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. Each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. Sensor nodes are small, low-cost, low power devices that have following functionality i.e. communicate on short distances ,sense environmental data perform limited data processing . Those are multifunctional. Their functionality depends on what sensors are attached. Sensor networks may consist of many different types of sensors such as seismic, low sampling rate magnetic, thermal, visual, infrared, acoustic and radar, which are able to monitor a wide variety of ambient conditions that include the followings [1]i.e. temperature, humidity, vehicular movement, lightning condition, pressure, soil makeup, noise levels, the presence or absence of certain kinds of objects, mechanical stress levels on attached objects, and the current characteristics such as speed, direction, and size of an object. Sensor nodes can be used for continuous sensing, event detection, event id, location sensing, and local control of actuators. The concept of micro-sensing and wireless connection of these nodes promises many new application areas.

II. KEY MANAGEMENT

Key Management includes the processes of key setup, the initial distribution of keys and key revocation (removal of the compromised key). To provide security, communication should be encrypted and authenticated. The open problem is how to bootstrap secure communications between sensor nodes, i.e. how to set up secret keys between communicating nodes? This problem is known as the key agreement problem. There are three types of general key agreement schemes: trusted-server scheme, self-enforcing scheme, and key pre-distribution scheme. The trusted-server scheme depends on a trusted server for key agreement between nodes, e.g., Kerberos. This type of scheme is not suitable for sensor networks because there is no trusted infrastructure in sensor networks. The self-enforcing scheme depends on asymmetric cryptography, such as key agreement using public key certificates. However, limited computation and energy resources of sensor nodes often make it undesirable to use public key algorithms, such as Diffie-Hellman key agreement or RSA, as pointed out in. The third type of key agreement scheme is key pre-distribution, where key information is distributed among all sensor nodes prior to deployment. If we know, which nodes will be in the same neighborhood before deployment, keys can be decided a priori. However, most sensor network deployments are random; thus, such a priori knowledge does not exist. There exist a number of key pre-distribution schemes, which do not rely on a priori deployment knowledge. A naive solution is to let all the nodes carry a master secret key. Any pair of nodes can use this global master secret key to achieve key agreement and obtain a new pair wise key. This scheme does not exhibit desirable network resilience: if one node is compromised, the security of the entire sensor network will be compromised. Some existing studies suggest storing the master key in tamper-resistant hardware to reduce the risk, but this increases the cost and energy consumption of each sensor. Furthermore, tamper-resistant hardware might not always be safe. Another key pre-distribution scheme is to let each sensor carry all secret pair wise keys, each of which is known only to this sensor and one of the other sensors. The resilience of this scheme is perfect because a compromised node does not affect the security of other nodes; however, this scheme is impractical for sensors with an extremely limited amount of memory because network size could be large. Moreover, adding new nodes to a pre-existing sensor network is difficult because the existing nodes do not have the new nodes' keysTo date, the only practical options for the distribution of keys to sensor nodes of large-scale distributed sensor networks whose physical topology is unknown prior to deployment would have to rely on key pre distribution. Keys would have to be installed in sensor nodes to accommodate secure connectivity between nodes. Security services such as authentication and key management are critical to secure the communication between sensors in hostile environments. As one of the most fundamental security services, pair wise key establishment enables the sensor nodes to communicate securely with each other using cryptographic techniques. Many Security-critical applications that depend on key management processes demand a high level of fault tolerance when a node is compromised. Another important thing is the size of key and amount of computation needed for that key while doing its operation. Thus we have to make a trade off between security and the available resources while designing an efficient key management scheme to achieve better security.

III. KEY MANAGEMENT SCHEMES

All key management schemes can be categorized in to two types i.e. pre distribution key management schemes where key information is distributed among all sensor nodes prior to deployment and in situ key management schemes those does not require keying information prior to deployment. This pre distribution can be divided into several categories based on Key Pool ,Random Pair Wise Key ,Key Space ,Group ,Grid , Deployment Knowledge ,Polynomial, Matrix Based, Tree, Combinatorial Design ,Hyper Cube ,Id ,Energy ,Location etc. Besides these categories of key pre distribution, there are several other probabilistic key pre distribution schemes place.

A.1 Pre Distribution Key Management Schemes

All key pre-distribution schemes must cope with the unpredictability of the network topology prior to deployment. Thus, a key pre-distribution scheme requires extra keying information to be pre-loaded in order to achieve desirable key-sharing probability between neighboring sensors. As a side effect, part of the keying information may not be utilized during the network lifetime. Further, this uncertainty can degrade the scalability of key pre distribution schemes.

A.2. Key pool based pre distribution key management schemes

In these schemes, a large key pool is computed offline and each sensor is preloaded with keys selected randomly without replacement from the key pool. These keys form a sensor's key ring. A pair of sensors can establish a secure communication channel as long as their key rings have at least one key in common. If there is no common key, a path key needs to be established with the help of an intermediary node that shares a key with each node in the pair. In 2002 Laurent Eschenauer and Virgil D. Gligor of Maryland University proposed a probabilistic key pre distribution scheme [2]. The main idea was to let each sensor node randomly pick a set of keys from a key pool before deployment so any two sensor nodes have a certain probability of sharing at least one common key. This scheme has three important features i.e. key distribution, revocation and re keying. This approach is scalable and flexible and is superior to the traditional key pre-distribution schemes. This scheme is assumed as the basic scheme in research field of key management of wireless sensor network security. In 2003 Haowen Chan ,Adrian Perrig and Dawn Song of Carnegie Mellon University further extended the idea of basic scheme and developed q-composite key pre distribution scheme[3]. The q-composite key pre distribution scheme also uses a key pool but requires two sensors compute a pair wise key from at least q pre distributed keys they share. By increasing the amount of key overlap required for key set up, the resilience of the network against node capture was increased. As the amount of required key overlap increases, it becomes exponentially harder for an attacker with in a given key set to break the link.In 2007 Ashok Kumar Das and Indranil Sengupta of Indian Institute of Technology, Kharagpur, India proposed a key establishment scheme suitable for mobile sensor networks for establishing keys between sensor nodes in an environment where the sensor nodes are highly mobile. They proposed it for mobile sensor networks with the help of additional auxiliary sensor nodes. This scheme supports efficiently addition of new nodes after initial deployment and also works for any deployment topology.The main idea behind this scheme is to deploy a small number of additional high end nodes along with a large number of low end sensor nodes in the network, so that high end sensors can help in pair wise key establishment procedure between sensor nodes.This scheme provides very high network connectivity as well as high resilience against node capture attack than the existing schemes and is highly applicable for mobile sensor networks. It also supports dynamic node addition after initial deployment. In 2010 Jianmin Zhang, Yu Ding of Henan Institute of Engineering, China developed a new key management scheme[4] using sub key pool to enlarge the size of key pool. The novelty of this approach is that before network deployment they use each key in the pool to generate a sub key pool using hash function. With more keys in the key pool the security level of against nodes, capture has improved. In that year Wenqi Yu of Henan Institute of Engineering, China presented an improved key management scheme for wireless sensor networks[5].In this proposed scheme the hash value of all keys is put in the key pool to form a new key pool. Keys in the key pool are called the original keys and the hash value of the original keys is called derivative keys. With the one way hash function, the proposed scheme can make attackers get less key information from the compromised sensor nodes.

A.3.Pair Wise Key Based Pre-Distribution Key Management Schemes

Random-pair wise keys scheme perfectly preserves the secrecy of the rest of the network when any node is captured, and enables node-to-node authentication and quorum-based revocation. In 2003 Haowen Chan ,Adrian Perrig and Dawn Song of Carnegie Mellon University proposed the Random pair wise scheme[3]. In the pre-deployment phase a total of several unique node identities are generated. The key is stored in both node's key rings along with the id of the other node that also knows the key. This scheme has a feature to revoke the entire key ring of any sensor node, when that sensor node is compromised. Distributed node revocation is possible by having neighboring nodes broadcast 'public votes' against a detected misbehaving node. If any node observes more than some threshold number of public votes against some node, then it breaks off all communication with that node. The random pair wise scheme possesses perfect resilience against node capture attacks as well as support for node based revocation and resistance to node replication. In 2009 Stephen Anokye, Thabo Semong, Qiaoliang Li and Qiang Hu of Hunan University, China made improvements on the Random pair wise scheme by Chang, Perrig and Song[6]. This scheme significantly reduces the memory and computational overheads and it has better connectivity. In that year Hung-Min Sun,Yue-Hsun Lin,Cheng-Ta Yang and Mu-En Wu proposed a novel pair-wise key establishment scheme[7]. It has several advantages i.e. it eliminates the path-key phase, the memory demand in this scheme is less, it enhances the security against node capturing attacks, it is flexible and it achieves fully connectivity without increasing storage requirement of sensors.In 2010 Sujun Li, Siqing Yang, Suying Zhu, Fuqiang Yan of Hunan Institute of Humanities, Science and Technology, China proposed a pair-wise key establishment scheme[8]. In this scheme, keys stored in a node which include two parts, the greater part are transformed by Hash function and the rest are come from the global key pool directly.

A.4.Key Space Based Pre-Distribution Key Management Schemes

Sensors pre-load multiple pieces of keying information, each of which belongs to a particular key space. Two sensors can compute a shared key if they have keying information from the same key space. However, the process involves expensive modular multiplications.In 2003 Donggang Liu and Peng Ning of North Carolina State University presented an instantiation of the key space based key management scheme[9]. This scheme consists of the following three components in the general framework.i.e. Subset assignment, Polynomial share discovery and Path discovery. In this scheme, sensors can be added dynamically without having to contact the previously deployed sensors. This scheme allows the network to grow. In that year Wenliang Du ,Jing Deng,Yunghsiang S.Han and Pramod K.Varshney proposed a pair wise key pre-distribution scheme[10].This has been built upon Blom's key pre distribution scheme and combines the random key pre distributions method with it . This key pre distribution scheme consists of three phases. I.e. Key Pre-distribution Phase, Key Agreement Phase and Computation of Memory Usage etc.This scheme has several important properties. I.e. it is scalable and flexible. It is substantially more resilient against node capture.

A.5.Group Based Probabilistic Pre-Distribution Key Management Schemes

Scalability issues, the Group-based schemes are proposed. Sensors are grouped based on IDs, and nodes with the same deployment group or the same cross group are preloaded with pair wise keys. Group-based schemes release the strong topology assumption that it adopts. The tradeoff for this flexibility exists in the form of higher communication overhead when two neighboring sensors try to establish a path key. In 2005 Zhen Yu and Yong Guan of Iowa State University proposed a group based key pre distribution scheme using sensor deployment knowledge [11]. In this scheme, a sensor field is partitioned into hexagonal grids. Sensor nodes are divided into groups. It scheme consists of a series of slightly different methods depending on how to distribute secret information among neighboring groups and how much information to be stored in each node. This scheme achieves a higher degree of connectivity of the sensor network with a lower memory requirement and offers a stronger resilience against node capture attacks. In 2006 Li Hui, Chen Kefei, Zheng Yanfei, Wen Mi of Shanghai Jiao Tong University, China presented an efficient key management scheme[12] for resource limited sensor networks. The idea behind this scheme is use secret sharing to distribute group key and manage group member as well as group header. This key management scheme is fully localized and do not need base station or other trust third party to be involved, which can save much energy consumption in communication.In that year Biswajit

Panja, Sanjay Madria and Bharat Bhargava described a group key management protocol for hierarchical sensor networks [13]where each sensor node generates a partial key dynamically using a function. The function takes partial keys of its children as arguments. The group key management protocol supports the establishment of two types of group keys; one for the nodes within a group and the other among a group of cluster head. The protocol handles freshness of the group key dynamically, and eliminates the involvement of a trusted third party. This scheme is able to compute the partial keys and the group key within a minor period. The energy consumption for generating the partial keys and the group key is very small compared to the total available energy. In 2007 Guorui Li ,Jingsha He and Yingfang Fu of Beijing University of Technology, china proposed a group-based dynamic key management scheme [14] in wireless sensor networks. In this scheme, there is no requirement for such infrastructure as base stations and cluster heads and the dynamic key update feature ensures the security of the network without tampering the compromised sensor nodes.Nahar Sultana, Ki Moon Choi and Eui-Nam Huh of Kyung Hee University proposed a group key management protocol also in 2007 [15] by introducing identity based infrastructure for secure communication in mobile wireless sensor networks. To ensure scalability and dynamic re configurability, the system takes a cluster based approach by which group members are broken into clusters and leaders of clusters securely communicate with each other to agree on a group key in response to membership change and member mobility events. This protocol has high probability to be resilient for secure communication among mobile nodes.In 2008 Ashok Kumar Das and Inranil Sengupta of Indian Institute of Technology,Kharagpur proposed a deterministic group-based key pre-distribution scheme[16]. This scheme guarantees that a direct key is always established between any two neighbor sensors in any deployment group.In this approach, it is efficient to replace a compromised group head node in a cluster by a new fresh group head node without affecting the existing sensor nodes in that cluster. This scheme has better performance in order to add fresh cluster head nodes as well as sensor nodes into an existing network and it possesses significantly better resilience against node capture and provides unconditional security against node capture. It is easy to deploy sensor nodes in a deployment group randomly by using this scheme.In that year Linchun Li, Jianhua Li, Yue Wu, Ping Yi of Shanghai Jiao Tong University, China proposed a group key management scheme for wireless sensor networks[17] in terms of the unreliable wireless channel and unsafe environment. This scheme implements node revocation through a broadcast polynomial to counteract the node compromise attack to provide a reliable communication. This scheme can efficiently revoke the compromised sensor nodes, implicitly authenticate the updated group keys and tolerate the key-update message loss under the unreliable wireless communication channel. Yugeng Sun, Juwei Zhang, Hao Ji and Ting Yang proposed a novel distributed key management scheme in 2008 [18] focusing on the management of encryption keys in clustered sensor networks. In this scheme, the sensor nodes are divided into some group, inner group pair wise keys are setup by a group key, and inter group pair wise keys. This scheme has some appealing properties i.e. it's key connectivity is high, is perfectly resilient against node compromise, and need less memory to store the keys. Shu Yun Lim, Meng-Hui Lim, Sang Gon Lee and Hoon Jae Lee proposed a new hybrid group key management scheme [19]for hierarchical self organizing wireless sensor network architecture also in 2008. By using this approach, multi-level security can be achieved to secure groups of sensors at different levels. They place the cryptographic burden where the resources are less constrained, at the forwarding nodes and the access points. In this scheme, access points and forwarding nodes initially perform a key agreement protocol and each sensor node in a cluster later on establishes a group key with the forwarding node using a key transport scheme dynamically after deployment. The key management scheme enables low-level sensor nodes to set up a cryptographic group key requiring only an initial secret and its static private key regardless of the network size. More promisingly, it is able to implement these encryption primitives in an efficient way without sacrificing their strength.Ting Yuan, Jianqing Ma and Shiyong Zhang of Fudan University, China proposed a random key management schemein 2008[20], which organizes sensor nodes into groups and uses multiple key pools to achieve higher security in large-scale sensor networks. This scheme divides the lifetime of the involved sensor network into a bounded number of deployment phases. All the sensor nodes to be deployed are organized into groups and are deployed within specific deployment phases. The key pre distribution and the group deployment introduced by this scheme relieve the side effect incurred by node capture attacks while ensuring a high intra-group and inter-group connectivity. This scheme is shown to be better resilient against node capture. In 2009 YingZhi Zeng , Yan Xia and JinShu SU proposed a group key management scheme [21]for wireless sensor network. This is an original scheme to the wireless sensor network for creating loop keys and their maintenance and renewing. It is feasible, efficient and secure for key establishment and maintenance in wireless Sensor Networks. This scheme is more balanced, cost saving, efficient and safe. In 2010 Guorui Li,Ying Wang and Jingsha He [22] proposed a Refined Key Link Tree (RKLT) scheme that incorporates dirty key path into the key link tree-based group key management scheme. By delaying key update operations in dirty key paths, the number of duplicate key update messages for auxiliary nodes can be reduced, which also brings down the energy cost. This scheme requires fewer re keying messages.

KunZhang and Cuirong Wang of Northeastern University at Qinhuangdao, China proposed a new group key management scheme[23] also in 2010. With grouping design and identity authentication of the nodes, this scheme improves the security connectivity and supports more large-scale networks. At the same time, the scheme reduces the node's memory overhead. This scheme suits wireless sensor network application which has upper security request.

A.6.Grid-Based Pre-Distribution Key Management Schemes

In 2005 Haowen Chan and Adrian Perrig of Carnegie Mellon University described Peer Intermediaries for Key Establishment (PIKE)[24]. It achieves a trade-off in both communications per node and memory per node. This scheme establishes keys between any two nodes regardless of network topology or node density. This makes it applicable to a wider range of deployment scenarios than random key pre distribution. This scheme enjoys a uniform communication pattern for key establishment, which is hard to disturb for an attacker. The distributed nature of this scheme also does not provide a single point of failure to attack. It has the advantage that key establishment is not probabilistic, so any two nodes are guaranteed to be able to establish a key.In that year Mohammed Golam Sadi, Dong Seong Kim, Jong Sou Park of Hankuk Aviation University presented an efficient framework[25] for establishing pair wise keys. The concept and analysis of this scheme explains its better improved resilience to node capture than the existing schemes along with a very high probability to establish pair wise keys between nodes in an efficient way. In 2006 R. KALINDI, R. KANNAN, S. S. IYENGAR and A. DURRESI of Louisiana State University, USA proposed a Sub-Grid based Key Pre-Distribution Scheme[26] for Distributed Sensor Networks. This scheme uses multiple mappings of keys to nodes. In each mapping, every node gets distinct set of keys, which it shares, with different nodes. The key assignment is done such that, there will be keys in common between nodes in different sub-grids. After randomly being deployed, the nodes discover common keys, authenticate and communicate securely. This scheme is able to achieve better security. In 2008 Nguyen Xuan Quy , Vishnu Kumar□ , Yunjung Park, Eunmi Choi and Dugki Min presented a grid-based scheme[27] .This scheme exploits new deployment knowledge and communication signal range of sensors. With such knowledge, each node only needs to carry a smaller number of keys while archiving a higher connectivity. This scheme also opens a new way for long peer-to-peer communication, where the increasing signal range does not lead to a much increase in the number of keys for each sensor.

A.7.Deployment Knowledge Based Pre-Distribution Key Management Schemes

Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen and Pramod K. Varshney developed a random key pre-distribution scheme [28] using deployment knowledge in 2004. The goal of this scheme is to allow sensor nodes to find a common secret key with each of their neighbors after deployment. This scheme has several important contributions i.e. node deployment knowledge has been modeled in a wireless sensor network, and a key pre-distribution scheme has been developed based on this model and it has shown that key pre-distribution with deployment knowledge can substantially improve a network’s connectivity and resilience against node capture, and reduce the amount of memory required. In 2007 Chun-Fai Law, Ka-Shun Hung and Yu-Kwong Kwok of The University of Hong Kong, China proposed a key pre distribution scheme[29] based on adaptability to post-deployment contexts, that exploits neighboring keys from connected neighbors to reach unconnected nodes and has several salient features, such as high connectivity, high resilience, and efficient memory usage. In 2008 Zhen Yu and Yong Guan, Member, IEEE proposed a novel key management scheme[30] using deployment knowledge. In this scheme, a target field is divided into hexagon grids and sensor nodes are divided into the same number of groups as that of grids, where each group is deployed into a unique grid. By using deployment knowledge, they drastically reduce the number of potential groups from which a node’s neighbors may come. Thus, a pair wise key can be generated efficiently for any two-neighbor nodes. This scheme achieves a higher connectivity with a much lower memory requirement and a shorter transmission range. In 2009 Paul Loree, Kendall Nygard and Xiaojiang Du presented an efficient post-deployment key management scheme[31] designed for heterogeneous sensor networks. The scheme does not assume any prior knowledge about sensor deployment and location. It takes advantage of a few powerful high end sensor nodes and achieves efficient and effective key establishment in a sensor network. This scheme has small communication, storage and computation overhead, and achieves strong resilience against the node compromise attack. In 2010 Juwei Zhang and Liwen Zhang of Henan University of Science & Technology, China proposed a routing-driven distributed key management scheme based on deployment knowledge (RDDKM)[32], which only establishes shared keys for neighbor sensors that communicate with each other. In this scheme, the sensor nodes are divided into some group, intra-group pair wise keys are setup only between the nodes which need to communicate with each other, and inter-group pair wise keys are established between cluster head sensors. This scheme has some appealing properties i.e. its key connectivity is high, is perfectly resilient against node compromise, need less memory to store the keys and cost less energy.

A.8.Polynomial Based Probabilistic Pre-Distribution Key Management Schemes

Ngo Trong Canh, Tran Van Phuong, Young-Koo Lee, Sungyoung Lee, and Heejo Lee presented a new key pre distribution scheme using bi variate polynomial combining with expected deployment knowledge [33]in 2007. This approach takes advantage in terms of resilience against node compromised. The pair wise keys in the setup phase are computed from the sharing key spaces between each two nodes. In 2008 Hu Tong-sen, Chen Deng, Tian Xian-zhong of Zhejiang University of technology, China proposed an enhanced polynomial-based key establishment scheme(EPKES)[34] for wireless sensor network. This scheme improves the security level of WSN. This scheme is scalable and flexible. New nodes can be very easily added, and session keys can be directly established with the existing nodes when needed. This scheme has a good key connectivity, scalability, direct key establishment, resilience to nodes capture and storage consumption. Hua-Yi Lin, De-Jun Pan, Xin-Xiang Zhao, and Zhi-Ren Qiu proposed a pre-deployment key management scheme[35] that requires a few memory capacities and CPU computations to address secure data transmissions in Wireless Sensor Networks in 2008. The proposed scheme exploits threshold key management mechanisms by Lagrange Interpolation polynomial generating a key set for sensor nodes, and uses symmetric and irreversible cryptography schemes to encrypt transmitted data by the generated keys with Message Authentication Code (MAC). The sensor nodes merely have to aggregate and encrypt received data without complicated cryptography operations. The proposed approach can achieve rapid and efficient secure data transmissions with low communications, and is proper to be implemented on large-scale sensor networks. In 2010 Min Li, Jun Long, Jianping Yin, Yongan Wu and JieRen Cheng of National University of Defense Technology,China proposed an efficient key management scheme[36] based on dynamic generation of polynomials for heterogeneous sensor networks which fully utilized the heterogeneity of sensor nodes. The scheme can support large scale heterogeneous sensor network because the polynomials which are used to compute the cluster keys are dynamically generated after deployment. Moreover, the renewal of keys is simple and convenient. The prominent feature of this scheme is that it didn’t need a key pool like traditional key management schemes. Polynomials are generated dynamically after deployment.

A.9.Matrix Based Pre-Distribution Key Management Schemes

Ting Yuan ,Shiyong Zhang and Yiping Zhong of Fudan University, China proposed a matrix based random key pre-distribution scheme[37] in 2007, which uses simple linear algebraic operations to derive common keys.In this scheme, they choose multiple key maps from the key map pool to assign initial keys to nodes. They do not have to exchange key indices in order for any pair of nodes to discover their common key set used for composing their session key. In 2008 Ni Chen, Jian Bo Yao and Gang Jun Wen of University of Electronic Science and Technology of China proposed an improved LU matrix key-distribution scheme[38] for wireless sensor networks based on the LU matrix, the hash function and the clustered structure. This scheme can keep the key connectivity with the network topology changes, delete and update key information with the network topology changes to avoid key information, reduce communication, computation and key storage overhead.

A.10.Tree Based Pre-Distribution Key Management Schemes

A.S.Poornima and B.B.Amberker proposed a tree based key management scheme for heterogeneous sensor networks[39] in 2008. This scheme handles various events like node addition, node compromise and key refresh at regular intervals and supports revocation of the compromised nodes and the energy efficient re keying. In that year Yi-Ying Zhang, Wen-Cheng Yang, Kee-Bum Kim, Myong-Soon Park of Korea University, Korea presented an AVL tree based dynamic key management[40] to enhance network security and survivability. This approach can efficiently protect the network against attacks of eavesdropping or captured nodes compromise, is adopted to address challenging security issues of runtime wireless sensor network. Even if the adversaries crack the sensor network keys, the entire network still remains safety under the timely protection of the re key mechanism. Also in 2008 H. M. N. Dilum Bandara, Anura P. Jayasumana, and Indrajit Ray of Colorado State University, USA presented a secure cluster tree formation algorithm[41]. This scheme is independent of key pre distribution, network topology, does not require apriori neighborhood information or location awareness and retains most of the desirable cluster and cluster tree characteristics while building the secure cluster tree. In 2010 Chih-Yu Lin of Asia University,Taiwan proposed a quadtree-based location management scheme[42] to overcome the limitations of traditional tree based key pre distribution schemes. The quad tree-based scheme does not need taking any statistics.Besides, this scheme benefits from low structure maintenance cost. In that year Khadija Rasul, Nujhat Nuerie, and Al-Sakib Khan Pathan of BRAC University, Bangladesh presented an enhanced heterogeneous tree based key management scheme[43]. This scheme combines efficiently different key management techniques in each architecture level and also it has a dynamic key renewal process. Here, whenever a node is compromised, key renewal is done by one way hash functions and simple XOR operations. Also in 2010

A.S.Poornima , B.B. Amberker , H.S.Likith Raj , S.Naveen Kumar , K.N.Pradeep and S.V.Ravithej proposed simple authentication schemes [44] based on tree based key management scheme and secret sharing. The proposed schemes identify malicious nodes acting as mobile agents and used to counter the various attacks launched by malicious nodes. These schemes identify malicious mobile data collector and replay messages. Transferred data is encrypted using refreshed secret key, which is known only to cluster head and base station.

A.11.Combinatorial Design Based Pre-Distribution Key Management Schemes

In 2005 Ling Tie, Jianhua Li of JiaoTong University,China proposed a new hierarchical key management scheme [45] for wireless sensor network based on a combinatorial optimization. This scheme provides a method for dealing with multiple participants leaving simultaneously by exclusion basis system. An important contribution of this scheme is that it yields optimal results for the number of re keying messages. In 2007 Seyit A. Çamtepe, and Bülent Yener, Member, IEEE presented novel deterministic and hybrid approaches[46] based on Combinatorial Design. Their approach is combinatorial based on Combinatorial Block Designs. They showed how to map from two classes of combinatorial designs to deterministic key distribution mechanisms, remarked the scalability issues in the deterministic constructions, and proposed hybrid mechanisms. The combinatorial approach produces better connectivity with smaller key chain sizes. It has following advantages i.e. it increases the probability of a pair of sensor nodes to share a key and decreases the average key path length while providing scalability with hybrid approaches. In 2010 Wenqi Yu of Henan Institute of Engineering, China presented a promising pair wise key establishment scheme. In this proposed scheme, after pair wise key establishment all attackers can't get any key information of uncompromised sensor nodes from compromised sensors. The novelty of this scheme is that it is combinatorial based on combinatorial design and attackers can't get any key information of non compromised sensor nodes from the compromised sensor nodes and the main advantage of this scheme is that the sensor networks are perfectly secure again sensor nodes capture after pair wise keys establishment. This scheme has better networks resilience against node capture attack.

A.12.Hypercube Based Pre-Distribution Key Management Schemes

In 2006 Wang Lei, Junyi Li, J.M. Yang, Yaping Lin, and Jiaguang Sun proposed a new security mechanism for key pre distribution by utilizing the properties of hierarchical hypercube model. This hierarchical hypercube key pre distribution scheme is based on some path key establishing algorithms. This scheme has lower communication costs, better performance and provides higher possibilities for sensors to establish pair wise key.In 2009 Zhao Huawei and Liu Ruixia presented a key management scheme [47] using hypercube model. The scheme solves two problems mainly: First, combining the structure of hypercube and two one-way functions, and giving an establishment scheme of pair wise keys. Second, designing an algorithm of finding neighbor nodes in the path of delivering cluster key, and when some sensor nodes in the path are disabled, cluster key also can be delivered efficiently in a cluster. The key storage of this scheme is lower, and secure connectivity is good. Fault tolerance is a character of their delivery method, and when some nodes in the delivery path are disabled, the active nodes in hypercube can also receive cluster key.In that year Yen Hua Liao, Chin Laung Lei, and Ai Nung Wang of National Taiwan University, Taiwan introduced a hypercube based pair wise key establishment for sensor networks .They improved the hypercube-based scheme based on this tame-based approach. It is able to fulfill fundamental authentication requirement in sensor networks, and still has the nice features of the hypercube-based scheme. Two sensor nodes need to find a key path for establishing an indirect pair wise key, if their hamming distance is bigger than one.

A.13.Id Based Pre-Distribution Key Management Schemes

In 2009 Zhiming Zhang, Jiangang Deng,Changgen Jiang of Jiangxi Normal University, China proposed a security and efficient key management scheme[48] by using node-ID and bilinear pairings for wireless sensor networks based on the network structure of clustering. This scheme establishes share secret key by using bilinear pairings, improves network connections, storage, communication burden and ability of resistance against node capture. In 2010 Zhang Li-Ping and Wang Yi proposed an ID-based pair wise key pre distribution scheme[49] for wireless sensor networks. In this scheme, the symmetric matrix is employed by hierarchical grid model to establish pair wise key. Different network zones possess different secret symmetric matrixes which is used to generate the key material. The proposed scheme improves considerably resilience to nodes compromising.

A.14.Energy-Aware Pre-Distribution Key Management Schemes

In 2003 Gaurav Jolly, Mustafa C. Kuscu, Pallavi Kokate, and Mohamed Younis of University of Maryland proposed a cryptographic key management protocol[50].This key management protocol is a symmetric-key mechanism, and consists of the sub-protocols. The approach does not call for any sensor to generate keys, or to perform any extensive computation associated with key management. The protocol supports the eviction of the compromised nodes. This approach supports key revocation and renewal mechanisms. In 2006 Bidi Ying, Huifang Chen, Wendao Zhao and Peiliang Qiu of Zhejiang University, China proposed an Energy-based Key Management (EKM) scheme[51]. This scheme stored identifier, residual energy and the pair wise keys into each node in the key pre distribution phase, searched for better secure links according to the identifier and residual energy, and then took multiplied times hash functions to implement the security for this scheme the view of the multi-hop communication. This scheme has lower energy consumption and longer the lifetime of the network, and reduces the probability of nodes capture. In that year Huifang Chen,Bidi Ying, Bo Chen, Hiroshi Mineno and Tadanori Mizuno improved the EKM key management scheme named the new scheme[52] as Low Energy Key Management (LEKM) . In this scheme, a key cluster consisting of multi continuous keys is stored into each sensor node in the key pre distribution phase, and then the secure network connection is searched based on the overlap of key clusters. The energy consumption is reduced and the security performance is enhanced in this scheme.In 2007 Jong-Myoung Kim, Joon-Sic Cho, Sung-Min Jung, and Tai-Myoung Chung of Sungkyunkwan University,Korea proposed an energy-efficient dynamic key management scheme[53] which performs localized re keying to minimize overhead.Since this scheme uses symmetric key between the base station and sensor node, it can authenticate the node and performs re keying more energy efficiently. The administrator of a specific wireless sensor network based on this scheme can select the proper metrics according to the network characteristics and the node characteristics.In that year Kwang-Jin Paek, Jongwan Kim, Chong-Sun Hwang Ui-Sung Song Proposed an Energy-Efficient Key Management Protocol(EEKM)[54]. This protocol supports the revocation of the compromised nodes and the energy-efficient re keying ,the broadcast-based re keying for low-energy key management and high resilience. For increasing complexity of encryption key, they use dynamic composition key scheme. Also in 2007 Tim Landstra, Maciej Zawodniok, S. Jagannathan of University of Missouri-Rolla, USA proposed a sub network key management strategy[55] in which the heterogeneous security requirements of a wireless sensor network are considered to provide differing levels of security with minimum communication overhead. Additionally, it allows the dynamic creation of high security sub networks within the wireless sensor network and provides sub networks with a mechanism for dynamically creating a secure key using a novel and dynamic group key management protocol. In 2009 C.Gnana Kousalya and Dr.J. Raja of Anna University, India developed a novel Traffic-Aware Key Management (EETKM) scheme[56] for wireless sensor networks, which only establishes shared keys for active sensors and participate in direct communication. This key management scheme achieves stronger resilience against node capture and low energy consumption.In that year Xing Zhang, Jingsha He and Qian Wei of Beijing University of Technology, China presented an energy-efficient dynamic key management scheme[57] in which new sensor nodes can join a sensor network securely and compromised nodes can be isolated from the network in time. This scheme does not depend on such infrastructure as base stations and robots, thus it possesses a high level of flexibility. In 2010 Lin HE, Yi-Ying ZHANG, Lei Shu, Athanasios V. Vasilakos and Myong-Soon PARK presented a new key management scheme named Energy-efficient Location-dependent Key Management scheme (ELKM)[58]. This scheme generates keys for each node based on their relative locations. Based on loose time synchronization, it reduces energy consumption significantly on the total size of transmitted message. This scheme guarantees high security level and good network connectivity.

A.15.Location-Based Pre-Distribution Key Management Schemes

In 2005Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang of China proposed the novel notion of location-based keys[59] for designing compromise-tolerant security mechanisms for sensor networks. This scheme has perfect resilience against node compromise, low storage overhead, and good network scalability. Another nice feature of this scheme is that, once finishing mutual authentication; two involved neighboring nodes have established a pair wise key indispensable for guaranteeing link layer security. In 2006 Cungang Yang ,Jie Xiao of Ryerson University Toronto, Ontario presented a novel key management and data authentication technique[60] that pass sensing data securely and filter false data out on its way to base station. The framework of this design is to divide sensing area into a number of location cells and a group of local cells consists of a logical cell.The established pair wise key is included in the message authentication code and is forwarded several hops down to the base station for data authentication. In 2007 Farooq Anjum of Telcordia Technologies proposed an approach for key management[61] in sensor networks, which takes the location of sensor nodes into consideration while deciding the keys to be deployed on each node. This approach is called as location dependent key management (LDK). This scheme starts with loading a single key on each sensor node prior to deployment. The actual keys are then derived from this single key once the sensor nodes are deployed. It allows for additions of sensor nodes to the network at any point in time, nodes to be added to the network anytime during the lifetime of the sensor network. In 2009 Mohammad Reza Faghani, S. M. Amin Motahari of Isfahan University of Technology,Iran proposed Sectorized Location Dependent Key management (SLDK). This scheme does not require any deployment knowledge of sensor nodes. Also sensor nodes can be added at any time to the network and are capable of establishing secure links with their neighbors. They tried to minimize the number of sub keys required to save.In that year Kaiping Xue, Wanxing Xiong, Peilin Hong, Hancheng Lu of China proposed a novel key management scheme [62]based on location to enhance the security of the wireless sensor networks. Here the location of a sensor node is described by its neighbors' logical identifiers. Taekyoung Kwon, JongHyup Lee and JooSeok Song, Member, IEEE developed a simple location-based pair wise key pre distribution scheme also in 2009. They call this scheme as full and random pair wise key pre distribution (FRP) scheme that uses deployment knowledge and path key offering method. This scheme is perfectly resilient to node capture. It shows much better performance with regard to path key connectivity and communications overhead, more storage efficient and more scalable. In that year Chunguang Ma ,Guining Geng ,Huiqiag Wang and Guang Yang of Harbin Engineering, University, China proposed a Location-aware and secret share based dynamic key management scheme[63] to effectively replace the compromised central node and enhance the security level of the network. Even the central node was compromised, it still can be quickly evicted and do little affection to the networks. They simplified the replacement of the central nodes, and the process of it is energy conserved.In 2010 In-Tai Kim, Yi-Ying Zhang, Myong-Soon Park of Korea University, South Korea proposed an efficient location dependent key management scheme[64]. In this scheme each pair of nodes find common keys by transmitting key indexes through successive applications of one-way hash function. Nodes generate keys depending on the location without any pre-deployment knowledge. The security effects of compromise ratio common keys through transmitting key indexes instead of all key materials while the security level does not degraded, but also message authentication is provided. In that year MinLi ,Jianping Yin and Yongan Wu of National University of Defense Technology, China proposed a localized key management scheme[65] for wireless sensor networks i.e. LEBKM . This scheme employs the localized strategy. The key for each node is integrated from two keys separately provided by other two key managements. It limits the impacts of betrayed node within a single cluster, which makes it can support large scale wireless sensor network. It can greatly enhance the resilience without changing the probability of secure connection. Hye-Young Kim and Young-Sik Jeong proposed a key management scheme[66] in sensor networks also in 2010 using an allocation of a location based group key for secure group communication. This scheme provides the revocation of compromised nodes and energy efficient re keying. It addresses the main function using a broadcast based re keying for low energy key management and high resilience.

A.16.Cluster Based Pre-Distribution Key Management Schemes

In 2004 Sencun Zhu Sanjeev Setia and Sushil Jajodia of George Mason University described Localized Encryption and Authentication Protocol (LEAP)[67], a key management protocol for sensor networks that is designed to support in-network processing. The design of the protocol is motivated by the observation that different types of messages exchanged between sensor nodes have different security requirements, and that a single keying mechanism is not suitable for meeting these different security requirements.This schemes supports the establishment of four types of keys for each sensor node. This scheme also includes an efficient protocol for inter-node traffic authentication based on the use of one-way key chains. A salient feature of the authentication protocol is that it supports source authentication.In 2008 Reza Azarderakhsh, Arash Reyhani-Masoleh, and Zine-Eddine Abid of The University of Western Ontario, Canada developed a key management in cluster based wireless sensor networks . The goal of this scheme is to introduce a platform in which public key cryptography is used to establish a secure link between sensor nodes and gateways. Instead of preloading a large number of keys into the sensor nodes, each node requests a session key from the gateway to establish a secure link with its neighbors after clustering phase. This scheme has significant saving in storage space, transmission overhead, and perfect resilience against node capture.In 2009 Qingqi Pei, Lei Wang, Hao Yin, Liaojun Pang and Hong Tang introduced a hierarchical key management scheme[68] based on the different abilities of different sensor nodes in the clustered wireless sensor network. In this scheme, the nodes are distributed into several clusters, and a cluster head must be elected for each cluster. Private communication between cluster heads is realized through the encryption system based on the identity of each head while private communication between cluster nodes in a same cluster head is achieved through the random key preliminary distribution system. In 2010 Yuan Zhang , Yongluo Shen and SangKeun Lee proposed a cluster-based group key management scheme[69] for wireless sensor networks that targets to reduce the communication overhead and storage cost of sensor nodes. In this scheme, a group key is generated by the collaboration of cluster head and nodes within the cluster. Only cluster heads take responsible for reconstruct and delivery the group key. This scheme maintains a good level of security while significantly reduced the communication overhead compared with the existing schemes, especially in a large-scale wireless sensor network. In that year Yao Nianmin,Ma Baoying and Fan Shuping proposed a clustering key management scheme[70]. Key update in this scheme large on inserting one single node. This scheme can ensure security of networks and reduce the communication traffic, lower network overhead, and prolong life cycle of networks. A.S.Poornima and B.B.Amberker proposed two schemes for key management[71] in clustered sensor networks i.e. Simple Secure Logical Ring (SSLR) and Burmester Desmedt Logical Ring (BDLR) also in 2010 . In SSLR scheme communication and computation cost incurred for key establishment is constant whereas in BDLR scheme key establishment is achieved by performing many multiplications and communications. These schemes establish key between the nodes of a cluster every time when the role of cluster head is changed.In these schemes without exchanging any additional information compromised node is revoked and new cluster key is computed.

A.17.Other Pre Distribution Key Management Schemes

In 2002 Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler and J. D. Tygar presented a suite of optimized security building blocks (SPINS) for resource constrained environments and wireless communication[72]. This model has two building blocks: SNEP and µ-TESLA. SNEP provides several security primitives i.e. data confidentiality, two-party data authentication, and data freshness and µ-TESLA provides authenticated broadcast for severely resource constrained environments. µ-TESLA is the micro version of the Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol. In 2004 Mohamed Eltoweissy, Mohamed Youois and Kajaldeep Ghumman proposed a new hierarchical key management scheme[73] for wireless sensor networks based on a combinatorial optimization of the group key management problem. Their solution uses symmetric encryption and re keying to support current, forward and backward secrecy.An important contribution of their solution is that it yields optimal results for the number of administrative keys per network granule and the number of re-key messages. In that year Ashraf Wadaa, Stephan Olariu, Larry Wilson and Mohamed Eltoweissy proposed a scalable key management scheme for sensor networks[74] consisting of a large-scale random deployment of commodity sensor nodes. In this key management scheme, any arbitrary subset of clone sets can be organized into a secure communication group. This protocol uses no communications, and thus is maximally efficient in terms of communications overhead. It scales well in the size of the network and supports dynamic setup and management of arbitrary structures of secure group communications in large-scale wireless sensor network. In 2005 Jaemin Park, Zeen Kim, and Kwangjo Kim of Information and Communications University (ICU),Korea proposed a novel random key pre-distribution scheme[75] that exploits new deployment knowledge, state of sensors, to avoid unnecessary key assignments and reduce the number of required keys that each sensor node should carry while supporting higher connectivity and better resilience against node captures. They expect to save of large memory space for each sensor node and also improvement of resilience against node captures. In 2006 Mohamed F. Younis, Kajaldeep Ghumman, and Mohamed Eltoweissy, Senior Member, IEEE proposed a novel distributed key management scheme[76] based on exclusion basis systems. This scheme is termed as SHELL because it is Scalable, Hierarchical, Efficient, Location-aware, and Lightweight. This scheme supports re keying and, thus, enhances network security and survivability against node capture. It distributes key management functionality among multiple nodes and minimizes the memory and energy consumption through trading off the number of keys and rekeying messages. It employs a novel key assignment scheme that reduces the potential of collusion among compromised sensor nodes. This scheme exploits the physical proximity of nodes so that a node would share most keys with reachable nodes. In 2007 Yi Qian, Kejie Lu, Bo Rong and Hua Zhu formulated the key management problem[77] as a multi objective optimization problem, in which the cost of the sensor network, and the security and survivability metrics of the sensor network are taken into account. To solve the multi-objective optimization model, they develop a genetic algorithm (GA) based approach that can efficiently obtain near optimal solutions. In that year Jamil Ibriq and Imad Mahgoub of Florida Atlantic University presented Hierarchical Key Establishment Scheme (HIKES) for wireless sensor networks[78]. In this scheme, the base station, acting as the central trust authority, empowers randomly selected sensors to act as local trust authorities authenticating on its behalf the cluster members and issuing all secret keys. It uses a partial key escrow scheme that enables any sensor node selected as a cluster head to generate all the cryptographic keys needed to authenticate other sensors within its cluster. This scheme localizes authentication and key distribution, provides one-step broadcast authentication mechanism ,defends the network against most known attacks. Amin Y. Teymorian, Liran Ma, Xiuzhen Cheng of George Washington University,USA developed a cellular automata (CA) based key management scheme[79] for wireless sensor networks termed as CAB also in 2007. This scheme allows sensors to establish pair wise keys during any stage of the network operation using pre-loaded cellular automata. A sensor computes pair wise keys with its neighbors after deployment by applying some initial parameters to their shared cellular automata. It has several nice properties i.e. it is computationally efficient, it achieves quasi-perfect resilience against node compromise and it is the first scheme that inherently provides re keying capabilities. In 2008 Qing Yang,Qiaoliang Li and Sujun Li proposed an efficient key management scheme[80] based on public key cryptography to establish distinct symmetric keys between communicating neighbor nodes. This scheme releases the assumption of prior knowledge of sensor deployment location. It preloads a small number of keys in more capable high-end sensors and utilizes Rabin’s scheme. It can significantly reduce sensor node memory and computation overheads. In that year Jiann-Liang Chen, Yin-Fu Lai, Hsi-Feng Lu and Quan-Cheng Kuo presented a public key based pre-distribution scheme [81] with time-position nodes for simultaneous exchange of secure keys. The proposed defend attack and key management mechanism for sensor network applications can successfully handle sink mobility and can continually deliver data to neighboring nodes and sinks. A node can detect jamming broadcast messages with the number of data packets arriving at the nodes exceeds an acceptable level and then switch to sleep mode instantly. The traditional cipher function with stream cipher is adopted to save code space, computational capability, power and memory. Quazi Ehsanul Kabir Mamun and Sita Ramakrishnan of Monash University, Australia presented two versions of a secured key management protocol in 2008[82]. This scheme uses partial key pre-distribution and symmetric cryptography techniques. Where as one version of this protocol uses shared partial keys in a sensor chain the other version uses private partial keys. The protocol outperforms other random key pre-distribution protocols in the sense that it requires lower space, lower communication overhead and offers very high session key candidates. Yoon-Su Jeong,Ki-Soo Kim,Yong-Tae Kim,Gil-Cheol Park and Sang-Ho Lee of KOREA proposed a protocol for wireless sensor network [83] in 2008.This scheme is more helpful in secure sessions established between sensor nodes and gateways. In the proposed protocol, efficiency was maximized by maintaining hop-by-hop routing function between sensor nodes using light weighted group key-based mechanism. In particular, an internal node plays a role of key management so that it can safely collect data with decreasing power load of sensor node, and that malicious action can be minimized in sensor network. In 2009 A.S.Poornima,B.B.Amberker and Harihar Baburao Jadhav proposed an energy efficient deterministic key establishment scheme[84] which ensures that always there exists a secret key between node and its cluster head. The proposed scheme is a deterministic scheme which establishes key in an efficient manner every time a cluster head is changed.. Storage at each node is optimized in this scheme. This scheme performs the task of establishing common key for node-to-cluster head communication in an efficient manner with respect to communication, computation and storage. Every time when a cluster head is changed key can be established by performing two transmit and two receive operations and it ensures that key can be computed between every node and its cluster head. In that year Huyen Thi Thanh Nguyen, Mohsen Guizani, Minho Jo, Member and Eui-Nam Huh proposed a probabilistic key pre distribution scheme [85] that guarantees a higher probability of sharing keys between nodes that are within the signal range than that of other schemes. Studying the signal ranges of the sensor nodes might significantly improve the performance of the key sharing mechanism. With such knowledge of signal range, each node needs to carry fewer keys, and achieve greater connectivity with less communication overhead and better resilience from diverse attacks. Manel Boujelben, Omar Cheikhrouhou,Mohamed Abid and Habib Youssef proposed a key management protocol[86] also in 2009 for heterogeneous sensor networks based on an asymmetric cryptosystem named pairing identity based cryptography. This protocol includes pair wise key establishment and also cluster keys and group key transport protocol. It assures key update and forward secrecy. This protocol has low communication and storage overhead. ZHANG Jian-hua and ZHANG Nan of Southwest University for Nationalities, China proposed a chaos scheme of key pre distribution and management in 2009[87]. In this scheme,the chaos over-spread character was used to enlarge the key space and increase the anti-decipher capacity. The chaos initial value sensitivity was used to spend smaller costs while greatly enhanced the security of system. This scheme was put forward based on the non linearity character of chaos, including inscrutability, inseparability, and initial value sensitivity, etc. In this scheme, the ergodicity of chaos was used to void the key of being decrypted, and chaos initial value sensitivity was used to ensure the key can be altered safely in communications. This scheme has advantage of small amount of computation, less energy consumption, low cost, and easy hardware implementation. Syed Muhammad Khaliq-ur-Rahman Raazi,Sungyoung Lee, Young-Koo Lee and Heejo Lee proposed an efficient key management scheme BARI also in 2009[88], which makes use of biometrics and is specifically designed for wireless body area networks (WBAN) domain. It provides required level of security in WBAN by exploiting the application characteristics of wireless body area networks. In 2010 Taogai Zhang, Hongshan Qu of Henan Institute of Engineering, China presented an lightweight key management scheme [89] for wireless sensor networks. In this scheme, hash function is used to alleviate the effect of compromised sensor nodes on the uncompromised sensor nodes and at the same time, this method does not affect the connectivity between neighboring sensor nodes. With the one-way hash function, this scheme can make attackers get less key information from the compromised sensor nodes. This scheme is substantially more resilient against sensor nodes capture. In that year Su Meibo, Yang Xiaoyuan, Wei Lixian and Yang Heng of Engineering College of Armed Police Force, ShanXi Xi'an designed a key management scheme [90], which is based on the geometric properties of circle. This scheme can guarantee that without changing the information stored in the nodes, it is possible to update the key. This scheme is simple, convenient and efficient; it has greater advantages in storage overhead, computation overhead, communication overhead and the dynamic topology. Beibei Kong, Hongyang Chen, Xiaohu Tang, and Kaoru Sezaki first used node's deployment knowledge to propose a hexagon scheme [91] in 2010, and then combine it with the bi variate-polynomial to realize a new key agreement scheme. This scheme achieves better local connectivity, stronger attack-resistant ability, and supports larger scale networks. Guohua Ou, Jie Huang and Juan Li proposed a key- chain based key management scheme [92] for heterogeneous sensor networks also in 2010. This scheme handles various events, such as pair wise key establishment, cluster key distribution and renovation. It released the assumption of prior knowledge of sensor deployment location. In this scheme, sensor only needs to be pre-loaded an initial key. It can significantly reduce the storage requirements, computation costs and support network extension or node mobility. Tao Liu and Ming-Zheng Zhou of An Hui Polytechnic University, China proposed a self-organizing key management scheme[93] based on trust model and Bilinear Pairing, called Behavior Trust-Based Keying (BTBK) in 2010. The administrative services provided by this scheme ensure the survivability of the network. According to behavior trust degree of the communicating node, this scheme provides security mechanisms including pair wise key establishment, update and revocation dynamically, which does not need base sites or special nodes. Bing ZHANG and Li CHEN of Suqian College, China proposed an improved key management mechanism [94] for large-scale ZigBee network in 2010. Based on the ZigBee public profiles; ZigBee is expected to be deployed in significantly large numbers of service application clusters for metering system as well as smart energy systems. This key management mechanism reduces battery cost, simplifies the key management procedures and has a better performance in resistance to the attack .

B. Insitu key management schemes

Sensors compute shared keys with their neighbors after deployment instead of pre-loading key information. Subsequently, the schemes all scale well with the size of the network and each of them can obtain a highly connected key-sharing graph with low storage overhead. However, a drawback of these schemes is that the shared key computation consumes a lot of energy compared to key pre-distribution schemes that do not employ random key spaces.In 2006 Fang Liu and Xiuzhen Cheng, Member, IEEE proposed LKE, a self-configuring in-situ key establishment scheme targeting large-scale sensor networks. This scheme employs location information for a deterministic key space generation and keying information distribution. For uniformly distributed networks, this scheme exhibits strong resilience against node capture attacks and achieves a high key-sharing probability. The design of this scheme targets large-scale sensor networks with severely constrained resources. In this scheme, sensors determine their roles and configure themselves automatically based on a pure localized algorithm. This scheme has a good performance in terms of key-sharing probability, keying information storage overhead, and resilience against node capture attacks.In 2007 Fang Liu,Xiuzhen (Susan) Cheng,Liran Ma and Kai Xing, Member, IEEE proposed an in situ self configuring framework[95] for bootstrapping keys in large-scale sensor networks. It does not require keying information. In this scheme, sensors differentiate their roles as either service nodes or worker nodes after deployment. Service sensors construct key spaces and distribute keying information in order for worker sensors to bootstrap pair wise keys. This scheme achieves good performance in scalability, key sharing probability, storage overhead, and resilience against node capture attacks.In that year Liran Ma, Xiuzhen Cheng, Fang Liu, Fengguang An and Jose Rivera proposed an in situ pair wise Key bootstrapping scheme for large-scale wireless sensor networks. The design of this scheme targets large-scale wireless sensor networks with constrained resources i.e.battery, memory, CPU etc. Worker sensors bear no key space information before deployment. They acquire keying pairs from service sensors in the neighborhood after deployment. This Scheme is more favorable when high-power service nodes are available in a heterogeneous sensor network. This scheme can achieve a high key-sharing probability between neighboring sensors and a strong resilience against node-capture attacks at the cost of low storage overhead.

IV. CONCLUSION

As each scheme was reviewed, the ability to analyze and comprehend the various key management schemes was proven to be a quite non-trivial task. Since many of the key management schemes are heavily based on mathematical computations, being a proficient researcher in this field requires a strong mathematical skill set covering such areas as calculus and discrete mathematics. Taking a step back, it was discovered that understanding the different deployments of wireless sensor networks could be considered a precursor to developing new or modifying existing key management schemes. We have seen that most of the probabilistic schemes are scalable in nature while most deterministic schemes are not scalable. However, deterministic schemes have the advantage of being simpler in terms of computation and they are better in terms of resiliency and connectivity because of its certainty. Schemes using basic schemes of Blom or Blundo et al have a good trade-off between security and storage. Schemes using combinatorial structures are good in terms of resiliency. In situ schemes require no preloaded keying information but let sensors compute pair wise keys after deployment. In situ schemes scale well to large sensor networks. We reviewed many key management schemes starting with the classic Eschenauer scheme and moving to the more recent schemes published in 2010. It is clear that numerous trade offs exist between different key management schemes, and the vast number of proposals make it difficult to compare them.

REFERENCES

[1]D.Estrin,R.Govindan,J.Heidemann,S.Kumar,Nextcentury challenges: scalable coordination in sensor networks, ACM MobiCom'99, Washingtion, USA, 1999,pp. 263–270.

[2]LaurentEschenauerandVirgilD.Gligour.AKeyManagement Scheme For DistributedSensor Networks.Inproceedingsof

the9thACMconferenceonComputerandCommunicationSecurity ,Pages 41-47,November 2002.

[3]H.chan,A.Perrig and D.Song, RandomKeyPredistribution Schemes ForSensorNetworks.InIEEESymposiumonSecurity andPrivacy,pages197213,Berkeley,CaliforniaMay1114,2003

[4] Pairwise Key Management Scheme Using Sub KeyPool for Wireless Sensor Networks By Jianmin Zhang,YuDingof HenanInstituteofEngineering,China2010SecondInternational Conference onInformationTechnologyandComputerScience.

[5]APromisingPairwiseKeyEstablishmentSchemeforWirelessSensorNetworksinHostileEnvironmentsByWenqiYuofHenan Institute of Engineering, China.

[6]StephenAnokye,ThaboSemong,QiaoliangLi,QiangHu,"GroupwisePairwiseSchemeforWirelessSensorNetworks," niss, pp.695-699, 2009 International Conference on New Trends in Information and Service Science, 2009

[7]A PairwiseKeyEstablishmentforWirelessSensorNetworks Found in: 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing By Hung-Min Sun , Yue-Hsun Lin , Cheng-Ta Yang , Mu-En Wu

[8]Anewpairwisekeyestablishmentschemeforsensornetworks BySujunLi; SiqingYang; SuyingZhu; FuqiangYan; DepartmentofComput.Sci.&Technol.,HunanInst.ofHumanities,Loudi,Chinain.ComputerApplicationandSystemModeling(ICCASM), 2010 International Conference .

[9] D. LiuandP.Ning,“Establishingpairwisekeysindistributed sensor networks,” in Proceedings ofthe10thACMConference onComputerandCommunicationsSecurity(CCS),Washington , DC, USA, October 27-31 2003, pp. 52–61.

[10] W. Du, J. Deng, Y.S.Han,andP.K.Varshney,“Apairwise key predistributionscheme for wireless sensor networks,” in Proceedings of the 10th ACM Conference on Computer and CommunicationsSecurity(CCS),Washington,DC,USA,October 27-31 2003, pp. 42–51.

[11]A robust group-based key management scheme for wireless sensor networks By Zhen Yu Yong Guan Dept. of Electr. & Comput. Eng., Iowa State Univ., Ames, IA, USA Wireless Communications and Networking Conference, 2005 IEEE.

[12] A_Locally_Group_Key_Management_withRevocationand Self_healing_Capability for Sensor Networks By LiHui;Chen Kefei;ZhengYanfei;WenMi;SystemsandNetworksCommunications, 2006. ICSNC '06. International Conference.

[13]Energyand communication efficient groupkey management_protocol_for_hierarchical_sensor networks by Panja,B.;MadriaS.K.;Bhargava,B.;SensorNetworks,Ubiquitous,andTrustworthyComputing,2006.IEEEInternationalConference

[14] A_Group_Based_Dynamic_Key_Management_Scheme_in Wireless____Sensor____Networks____By GuoruiLi; JingshaHe;YingfangFu;AdvancedInformationNetworkingandApplications Workshops, 2007, AINAW '07. 21st International Conference

[15] ApplicationDrivenClusterBasedGroupKeyManagement with Identifier in MobileWirelessSensorNetworkBySultana, N. Ki Moon Choi Eui-Nam Huh Kyung Hee Univ, Seoul in Future Generation Communication and Networking (FGCN 2007)

[16] Ashok Kumar Das and Indranil Sengupta “AnEffective Group-Based Key Establishment Scheme for Large-Scale Wireless Sensor Networks using Bivariate Polynomials”.

[17] A Group Key Management Scheme with Revocation and Loss-tolerance Capability for Wireless Sensor Networks ByLinchunLiJianhuaLiYueWuPingYiin: PervasiveComputing and Communications, 2008. PerCom 2008. Sixth Annual IEEE International Conference

[18] KMSGC:_A_Key_Management_Scheme_for_Clustered WirelessSensorNetworksBasedonGrouporientedCryptography Yugeng Sun; Juwei Zhang;HaoJi;TingYang;Networking, Sensing and Control, 2008. ICNSC 2008. IEEEInternational Conference .

[19] Secure_Hybrid_Group_Key_Management_forHierarchical Self_Organizing__Sensor__Network__ByShuYun LimMeng HuiLim ; Lee, S.G.; Lee, H.J.; in ISIAS’08.

[20] Random_key_management_using_group_deployment inlarge-scale sensor networks Ting Yuan,Jianqing Ma ShiyongZhang.

[21]A_new_group_key_management_scheme_based_on_DMST for Wireless Sensor Networks YingZhi Zeng; Yan Xia; JinShu Su in MASS’09.

[22] Efficient_Group_Key_Management_Scheme_in_Wireless Sensor_Networks_By Guorui Li; Ying Wang; Jingsha He in (IITSI), 2010 .

[23] A_new_Group_Key_ManagementSchemewithsimplehash based_ authentication for wireless sensor networks KunZhang ; Cuirong Wang; in ICCDA, 2010

[24] PIKE: peer_intermediaries_for_keyestablishmentinsensor networks_ByHaowen Chan; Perrig,A.;inINFOCOM 2005.

[25] GBR: Grid Based Random Key Predistribution for Wireless Sensor Network BySadi, M.G. Dong Seong Kim Jong Sou Park Comput. Eng. Dept., Hankuk Aviation Univ. Parallel and Distributed Systems, 2005. Proceedings. 11th International Conference .

[26] Sub-Grid based Key Vector Assignment:A Key Pre Distribution Scheme For Distributed SensorNetworks(2006) By R. KALINDI, R. KANNAN, S. S. IYENGAR and A. DURRESI of Louisiana State University, USA.

[27] A_High_Connectivity_Pre-Distribution_KeyManagement Scheme_in_Grid-Based_ Wireless Sensor Networks_By Nguyen Xuan Quy; Kumar, V.; Yunjung Park; Eunmi Choi; Dugki Min in ICHIT'08.

[28] Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen and Pramod K. Varshney ,"A key Management scheme for wireless sensor networks using Deployment knowledge" appered in IEEE INFOCOM'04.

[29] A_Novel_Key_Redistribution_Scheme_forWirelessSensor Networks_By Chun-Fai Law;KaShunHung;YuKwongKwok; Communications, 2007. ICC '07.

[30] A_Key_Management_Scheme_Using_Deployment Knowledge_for_Wireless_Sensor_Networks_By Zhen Yu; Yong Guan; Parallel and Distributed Systems.

[31] An_Efficient_Post-Deployment_Key_Establishment Scheme_for_Heterogeneous_Sensor_Networks_By Loree, P.; Nygard, K.; Xiaojiang Du; GLOBECOM 2009. IEEE .

[32]Aroutingdrivenkeymanagementschemeforheterogeneous wireless_sensor_networks based on deployment knowledge ByJuweiZhang;LiwenZhang;IntelligentControlandAutomation (WCICA),2010s.

[33]ALocationawareKeyPredistributionSchemeforDistributed_Wireless_Sensor_Networks_By Ngo Trong Canh; Tran Van Phuong; YoungKooLee;SungyoungLee;HeejoLee in ICON'07,IEEE.

[34]AnEnhancedPolynomialBasedKeyEstablishmentScheme_for_Wireless_Sensor_Networks_By HuTongsen;Chen Deng; Tian Xian-zhong; Education Technology and Training, in ETT and GRS 2008.

[35] A_Rapid_and_Efficient_Pre-deployment_Key_Scheme_for Secure_DataTransmissionsinSensorNetworksUsingLagrange Interpolation Polynomial_By Hua-Yi Lin; De-Jun Pan; Xin-Xiang Zhao; Zhi-Ren Qiu;in ISA 2008.

[36] An_efficientkeymanagementbasedondynamicgeneration of_polynomials_ for heterogeneous sensor networks_By MinLi; Jianping Yin; Long, J.; Yongan Wu; JieRen Cheng;in ICCET,2010.

[37] A_Matrix-Based_Random_KeyPredistributionSchemefor Wireless_Sensor_Networks_By Ting Yuan; Shiyong Zhang; Yiping Zhong; in CIT 2007.

[38] A_LU_Matrix-Based_Key_Pre-Distribution_Scheme_for WSNs_By Minghui Zheng; Huihua Zhou; Guohua Cui;in WiCOM'08.

● ● ●