Improved Key Distribution and Management in Wireless Sensor Network

Vishal Choudhary, S. Taruna

Abstract—Key set up and distribution in sensor network is a complex task due to inherent limitations in sensor networks. For reducing the “communication and computation overhead” we proposed that the sensor network is partitioned into different zones. Each zone has a separate intrusion detection system (IDS) and key distribution center (KDC). IDS can detect the activity in its area and communicate with its KDC. KDC is controlled by the base station. Our main concern is that how to make a secure link in between KDC to sensor nodes and KDC to the Base station. Here we will try to reduce the computation and communication overhead of the already overloaded base station by separating the intrusion detection work of the base station with a separate entity in each zone.

Keywords—key distribution; sensor network security; key management protocols; intrusion detection; cryptography.

I. INTRODUCTION

Advancement in sensor network technologies gives new challenges in the field of control and key communication management. Also there are many limitations while dealing with sensor networks like their size, communication range, processing and storage power, deployment limitation. In addition to these limitations, security is the main issue and extensively studied in the literature for many years. In traditional networks, communication media is wired also storage and processing power of network devices are huge, so traditional protocols create no problem in these networks. But in sensor networks, there is a need of alternate protocol which runs smoothly without any trouble in the overall architecture.

Security in wireless sensor network faces some major challenges due to wireless communication, resource limitation, in permanent topology as well as limitation in adaptation of existing protocols. The unreliable communication links makes the security defense system even harder. For general purpose sensor networks, it is an assumption that all nodes are reliable, but this is not true in case of many sensor network applications. Now the center of attention is on, “building a sensor trust model that solve the problems ahead the capacity of cryptographic security. here our focus is on key management and distribution in sensor networks. Cryptographers, security experts invented several key management protocols that provide secure exchange of data between sensor nodes and base stations, but each one have some drawbacks. Basic idea is to secure distribution of “secret keys” in between “communicating nodes”. The key distribution and management protocols are divided in two different categories based on their characteristics. The recent survey demonstrates that “pre-loading the keys into sensors memory before their deploys is a convenient technique” (Adrian Perrig et.al.) [1]. But it is good only when the network size is small up to 100 nodes. In real applications sensors network deploy thousands of nodes. Pre-loading of keys is possible in two ways. In first approach, also known a master-key method, for which all nodes are “pre-loaded with single symmetric key in its memory” and after the network deployment, every pair of “nodes in the network” uses the same “symmetric key to encrypt/decrypt” the information in between them. It may be a suitable technique due to the reason that operating cost for key establishment is negligible and requires only “single key to be stored” in each sensor node. But the central limitation in this procedure is that, even a single node capture direct to compromise of entire network. Also, manual loading of keys in each sensor is overhead and time consuming. Alternative to master-key approach is “pair wise key based approach” Rodrigo Roman et.al. [2]; in this a group of “symmetric keys” are preloaded in all sensors memory to make confident that; “any two nodes have a distinct key between them”. This technique imparts adequate security. Any node capture cannot negotiate the “safe communication between non-captured” entities. But this technique is “not scalable due to its exceedingly
large key storage space overhead”. Another approach known as, “random key distribution “L. Eschenauer, V. D. Gligor [3]” has no computational overhead to generate pair wise keys between sensor nodes. But there is a large communication overhead for shared key discovery phase and is proportional to the number of keys stored in each sensor. So still there is tradeoff in between network connectivity and key storage space. Polynomial-key pre-distribution “Lee and Stinson [4]” have lower message overhead than random key distribution, but cannot provide adequate security for large networks against the node capture attacks. In order to reduce the communication and computation, operating cost we proposed that the sensor network is partitioned in to different zones. And each zone has a separate intrusion detection system and key distribution system”.

In this paper, however, we proposed that the sensor network is partitioned into different zones. Each zone has a separate intrusion detection system (IDS) and key distribution center (KDC). The proposed scheme reduces the computation overhead of base station as key distribution and intrusion detection is separated into different entities. The rest of paper is organized as follows: Section 2 highlights the related work. Section 3 describes the framework for proposed scheme. Section 4 gives the proposed algorithm. Finally, Section 5 concludes the paper.

II. RELATED WORK

Adrian Perrig et al. published a paper in the ACM journal on security protocol for wireless sensor network (Adrian Perrig et al.)[1] in which they adopted the simplest technique for key distribution “where they pre-load a single key into all nodes ahead of deployment. In their technique there is no need for nodes to carry out the key discovery or key exchange as all nodes share the same key. The main problem with their technique is that even single node conciliation leads to compromise of whole network through the shared key. The alternative to single key is that, each node in the sensor network assigned a different key for communication with each other, but main problem is the reduced scalability. That is the number of keys that are stored in each node is relative to the total quantity of nodes in the network”.

L. Eschenauer, V. D. Gligor [3] published a paper "Key management scheme for distributed sensor networks in the proceeding of the 9th ACM Conference on Computer and Communication security (2002)", in which a , “random key probabilistic distribution schemes is devised on the basis of random graph theory. A random graph is created by starting with a set of n vertices as nodes and adding edges as links between them at random way, a random graph is indicated by G(n,p), in which each feasible edge occurs autonomously with probability p. In order to achieve full graph connectivity, every pair of vertices need to have relatively lower probability P0 for existence of direct link. When sensor nodes are deployed, a key-setup phase is performed. During this phase all the nodes discover their neighbor and share the unique key. Key searching can be done by assigning a small identifier to every key before deployment. The nodes which notices that they include a shared key in their key rings can verify their neighbor by challenge and response protocol. The shared key then act as a key for that link”.

Du, Deng, Han and Varshney [5] published a paper in the "Proceedings of IEEE 2003 Global Communications Conference (2003)” in which they proposed a pair wise keying model, their model is an extension of Schauzer and Blom's research, but as a replacement for “individual keys it uses with array of keys. Blom's model depends on the symmetric matrix multiplication, where row i column j is equal to row j column i. Thus when node i calculates key pair ij and node j calculates key pair ji then keys are alike, leads to a common shared secret. In Du's pair wise key management proposal, as an alternative of using only one secret matrix, the sink node generates i private matrices, in addition every node contains a small set of these matrices in same way as Eschenauer's key ring. When two nodes communicate, they initiate by broadcasting the node Ids, the index of key matrices and the starting point of the column of the public matrix. If there is a common key matrix, then they can compute the pair wise secret key using Blom's Scheme. It offered strong toughness against node compromise at a practical scalability cost. In this proposal, it is considered that opponent must compromise five times as many nodes in comparison with Eschenauer's scheme to compromise the complete network. But the complexity of protocol increases the overhead. Since it does not use pair wise key, neither key revocation nor key refreshing are considered”.

Panjna, Madria, Bhargava[6] published a research paper in the proceedings of “the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (2006)”their protocol is similar to, “hierarchical group keying scheme by use of Tree-based Group Diffie-Hellman (TGDH) protocol”. The TGDH keying scheme has one level of universal sensor nodes and many levels of cluster heads, each cluster head is manager for various cluster head under it. The main benefit of this method is that it is straightforward and hence, “simple to implement, less computational and storage cost, key revocation and refreshing problems are solved”.

S. Zhu, S. Setia, and S. Jajodia[7] published a paper “efficient security mechanisms for large-scale distributed sensor networks in proceedings of the 10th ACM conference on Computer and Communication Security (2003)” in which they described a scheme that
is based on, “Initial Trust model, here each node share a universal master key K as well as a keyed hash function H. After deployment nodes initiate discovery of all adjacent nodes and establish pair wise key using K and H. For example, the pair wise key between node X and Y can be $H_K(X|Y)$. After establishing every pair wise key, all nodes relinquish the master key, in this scheme it is assumed that time needed for an adversary to compromise a node is greater than the upper duration of nodes to complete the key distribution, if this theory holds true then this scheme is secure, however the sensor deployment took place in different phases and new sensor needs to be deployed when previous deployed sensor fails. The new nodes cannot create pair wise keys with previous nodes. So it will not support multi-phase deployment. Example of such scheme is Localized Energy-Aware Prediction. If sensor nodes are sprinkled from airway, then the nodes may settle very far from each other so need adequate time to create the network and launch pair wise keys. For this duration, an enemy can capture a sensor node and obtain an initial key”.

R. D. Pietro and J. Radhakrishnan[8] presented a paper on “Connectivity properties of secure wireless sensor networks in the 2nd ACM workshop on Security of ad hoc and sensor networks (2004)” in their proposal, “sensor nodes are randomly deployed and there is large number of nodes. we may think of a WSNs as a graph, sensor nodes a vertices and links as edges. This scheme works as follows. Let m be the number of distinct cryptography’s key that can be stored on a sensor. Ahead of deployment, an offline trusted key sharing server produce a key group of S random keys out of total feasible key space; keys are randomly chosen from the key group and loaded into nodes memory”.

M. Eltoweissy et.al.[9] published a paper “Group key management scheme for large-scale sensor networks in the ACM journal of Ad Hoc Networks (2004)” in which they published, “efficient group key management schemes for dynamic system. Various conventional binary-tree-based cluster key management schemes and broadcast methods, example for logical key hierarchy, one-way function chain tree and subset-cover broadcast encryption can be used into wireless sensor network. In order to reduce the agreement among compromised sensor nodes in standard EBS system, Eltoweissy[29] proposed SHELL scheme, using node position information to calculate keys with the assistance of clusters and gateways. SHELL scheme collect information about node locations after deployment and uses these values for assigning keys. SHELL exploits the physical proximity of nodes so that they can share the majority of keys with accessible nodes, and very few supplementary keys would be exposed when they want to collaborate. In this model, each group has its personal distributed key management unit residing in a non-clustered header node. The operational and key management jobs are divided leading to better resistance against node capture”.

B. Sunar et.al[10] presented a paper “Public key cryptography in sensor networks in the first European Workshop on Security in Ad-Hoc and Sensor Networks (2004)” in which they discussed the common perception about, “public key cryptography on sensor network that public key cryptography is very complex, slow, consume more power. It is observed that use of right selection of algorithms and related parameters; optimization and low-power design techniques make the public key cryptography possible for wireless sensor networks”. Smith et.al.[11] (2004) in “First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (IEEE SECON 2004) proposed the first practical implementation of elliptic curve cryptosystem for sensor networks”.

Seiy A. C, antmebe, Bulent Yener[12] published a paper “combinatorial design of key distribution mechanisms for wireless sensor networks in the IEEE/ACM Transactions on Networking (2004)” in which they given first proposal of “deterministic methods with combinatorial design in key distribution, they showed realistic view to map from two module of combinatorial designs, that is unbiased block designs and another generalized quadrangles to achieve deterministic key distribution scheme”. Roy et.al[13] presented a “randomized block integration policy” for key “pre-distribution in WSNs”. Yuguang Fang[14](2005) described the improved version of random key distribution, since the “sensor nodes are randomly spread into particular area, thus it is hard to acquire deployment information of sensor nodes. The major issue is how to build up suitable node deployment model. The deployment knowledge is modeled by Wenjing Lou and Yuguang Fang using non-uniform probability density functions which assume the position of sensor nodes to be at certain areas. Since the nodes are set out in groups. Therefore the probability density function of the final resident point of all the sensors in group is expected to be same in comparison with the group of sensors deployed in a single deployment spot. Doyle et.al.[15] used efficient elliptic curve and identity-based encryption algorithms to set up a secure sensor network”.

Traynor et al.[16] published a paper “Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks” in the IEEE Transaction on Mobile Computing (2007) in which they discussed, “a random key distribution design based on the heterogeneous network model. In this model sensor nodes are assumed to be overloaded with a fast encryption/deletion algorithm to defend their ancillary keys from compromise under the circumstances if they
are captured. Based on this a scheme for the heterogeneous allocation of keys all over a wireless sensor network with more dominant nodes in a sensor network better security can be achieved”.

Lee and Stinson[17] published a paper in the “ACM Transactions on Information and System Security (2008) where they suggest the deployment of the set of linear and quadratic polynomials, for improving the performance of key pre-distribution”.

Piotr Szczechowiak et.al. [18] presented a paper on “NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks in the 5th European Conference (2008)”, they updated results of their research by “implementing ECC, and PBC, over MICA2 and Tmote Sky nodes, they demonstrated that these types of PKC are not only feasible, but in fact also practical for resource constrained sensors. They present results on point multiplication and pairings”.

Wen Hu et.al.[19] presented a paper on “secFleck: A Public Key Technology Platform for Wireless Sensor Networks” in the 6th European Conference (2009)”, for “hardware based implementation of Public Key Cryptography (PKC) on secFleck platform, which includes a standard Trusted Platform Module( TPM)chip and a set of software primitives for supporting Public Key Cryptography (PKC) in a WSN. According to them secFleck is the initial platform that supports the majority of RSA-based PKC functions in WSN”.

T.Kavitha et al.[20] published a survey paper in the “Journal of Information Assurance and Security (2010)”, in which they reviewed “the classic attacks on sensor networks on many important security issues related to the sensor networks, including key administration, secure time management, secure location discovery”. Alert message transferred to the base station, if it fails to communicate with the nodes. McCusker, K. and N. O’Connor [21] published a paper “Low-energy symmetric key distribution in the wireless sensor networks in IEEE Transactions on dependable and secure Computing (2011) in which they proposed the key assignment in to different phases. In first phase of the scheme is concerned with allocating the domain parameters and private keys to the nodes. The elliptic curve as well as Galois fields being used is hard coded on the device”. In “second phase symmetric keys are set up between neighboring nodes in a pair-wise fashion. The nodes would transmit a small signed message to each device in radio range at time T1. That is devices that can generate a legitimate signature are permitted to join the network. In third phase known as time T3 extra devices may be added to the WSN. At a previous time T2 the key generation center (KGC) broadcast though the network the identity of the nodes to be added, e.g. EKGC = \{Q_0, Q_p\}. The identities of these entire sensors with a timestamp are verified by the KGC. It does this in order to validate these identities and avoid the message requesting the addition of these identities being played back by an adversary in the future”.

Rodrigo Roman et.al.[22] highlighted about Key management system, in their paper “first step for network designer is to create a key pool, which is set of pre-calculated secret keys”. In “second phase before the network deployment every node is allocated with a distinctive key chain, i.e. a small subgroup of the keys from the key group”. In “third phase, after the network deployment, the sensor nodes exchange their identification number of the keys from their key chains, trying to discover a common shared secret key”. At last, “in case two nodes do not share the same key, they try to find a secure routing path between them in order to negotiate a pair wise key”.

Xing Zhang et.al.[23] proposed, “an energy-efficient distributed deterministic key management scheme (EDDK)” in which pair wise keys and neighboring “cluster keys of nodes can be established and maintained” safely, here pair-wise keys are entirely decentralized. The negotiation of any “sensor node will not affect any other non-compromised pair wise keys, with transmission of only one identity authentication message, a node can lay down a pair wise key with an adjacent node both in the network initialization phase and in the mobility scenario”. As a result, communication, operating cost negligible.

Leonardo B et al. [24] in their research paper point towards, “Identity Based Non-Interactive Key Distribution Scheme”. In their research two nodes only knows each other’s identity, rest everything is secret. Each entity gets its “distinctive secret from trusted authority known as organizer of network. This will generate the exclusive secret from nodes’ IDs and a master secret of its personal data”.

Wang Wei, Wang Zhaoba [25] proposed a new location encryption modulation algorithm RSSI-AM based on the RSSI sensor network, known transmission and receiving powers’ uses receiving power loss of receiving node to calculate transmission loss, it turns transmission loss into distance by applying signal transmission model. After obtaining appropriate distance information between anchor nodes and unknown nodes, adopt trilateral or maximum likelihood estimation technique to get the location of unknown nodes.

Walid Abdallah et.al. [26]investigated, “the design of an efficient key distribution and management proposal for sensor networks. Their proposal is based on the creation and allocation of different encryption keys projected to secure individual and group communications. Andrew Newell et.al.[27]focused on
ensure secrecy and reliability of key establishment. Secrecy ensures that only the two parties establishing the key have knowledge about the key. Integrity ensures that nodes that already captured do not alter the keys being established; here the network administrator first initializes each sensor with a group of secret keys selected from a large pool, then the sensor nodes are spread randomly and uniformly in the test bed, after that the sensor nodes search their physical neighbors determined by a fixed communication range, neighbors try to establish a secret key by using their pre shared keys and communicating with other nodes over multi-hop paths, according to this paper coding over multiple paths can achieve higher resilience for compromised nodes than other schemes. Various path put forward different group of transitional nodes that act to forward key information. The coding procedure ensures that the confidentiality and reliability of the shared key is preserved despite certain paths being under attack. Particularly, if less than half of the paths have a compromised node, then the coding is successful; else, the enemy could smash confidentiality, integrity, or both”.

Lein Harn et.al. [28] proposed, “a scheme, in which mutually trusted key distribution center over n sensors \( \{U_1, U_2,..., U_n\} \). Each sensor is to pre-load share key by a key distribution center. The key distribution center selects a special type of m-variate polynomial and generates key groups. Shares of every sensor are \( m-1 \) uni-variate polynomials. In order to set up a secure cluster communication involving m (i.e. \( 2 \leq m \leq n \)) sensors, the group key is computed by each sensor using its shares. There is no relation with other sensors to calculate the group key. In their view proposed method is very competent in group key establishment since there is no extra communication overhead. Besides, the group key calculation of each node needs only polynomial calculation which is much quicker than public-key calculation”.

Seung-Hyun Seo et.al.[30] Gives the idea of certificate less Public/Private Key where, “prior to node deployment, the key generation center (KGC) at the base station create a unique certificate less private/public key pair and fix the keys in the node. This key pair is used to produce a mutually authenticated pair wise key. Each node shares a distinctive individual key with Base station.e.g. A nodes with low processing capabilities (L-sensor) can use the unique key to encrypt and with high processing capacity( H-sensor). An H-sensor can use its keys to encrypt the message equivalent to changes in the cluster. The base station can also use this key to encrypt susceptible data, such as compromised node information. Before a node is deployed in field, the base station assigns the node with unique key. Every node shares a different pair wise key with each of its adjoining nodes for securing the communications as well as for authentication of nodes. e.g. in order to join a cluster; an L-sensor must share a pair wise key with the H-sensor. Then, the H-sensor can safely encrypt and allocate its cluster key to the L-sensor by using the pair wise key. In the aggregation, supportive sensor network, the L-sensor can use its pair wise key to securely broadcast the sensed data towards H-sensor. Each node can dynamically launch the pair wise key between itself and another sensor node by the use of their individual certificate less public/private key pairs. Each node in a cluster share a key, named as cluster key. The cluster key is mostly used for securing transmitted messages in a cluster, e.g., sensitive commands or the change of member value in a cluster. Only the cluster head can renew the cluster key when L-sensor leaves or joins the cluster”

III. A FRAME WORK FOR KEY DISTRIBUTION IN WIRELESS SENSOR NETWORK

An attacker can join or “try to join the network and be a component of genuine nodes of the network”. Also there exist “numerous intrusion detection techniques (IDS) in the literature which is used to detect suspicious behavior .an IDS either looks for, malicious activity in the network or monitors the internal activities of nodes”. If the IDS detect any malicious activity in the network it will communicate with key distribution center(KDC).now it’s the responsibility of the KDC and base station to take the decision for update the keys used by all the sensor nodes with in a cluster head or within a particular coordinates. To update all the keys in the entire network is communication and computation overhead. In order, “to reduce the communication and computation overhead”. We proposed that the sensor network is partitioned in to different zones. And each zone has a separate intrusion detection system. Each IDS can detect the activity in a particular area. In our proposal, we partitioned the networks in X, Y and Z Co-Ordinates and each sensor node is uniquely identified by its coordinate and identifier number. The effectiveness of any key distribution system depends on how fast computation and communication takes place. The effectiveness and consistency of an algorithm on resource constrained network ultimately leads to a versatile sensor network. In literature, we examined many techniques but each one have some advantages and disadvantages. To overload the entire computation on single nodes creates the bottleneck in the system. Hence in our work we are inspired to create a system which can effectively use the previous studied algorithm plus additional modification in the topology of sensor network. In our study we will focus on either sensor to sensor or sensor to cluster head authentication is effective. If the IDS of one zone fails to detect the intrusion then how other zone IDS communicate with KDC, we have to decide on what parameters KDC took the decision for key updating and revocation of sensor nodes.
IV. PROPOSED ALGORITHM & FLOWCHART

The key distribution and revocation algorithm is outlined as follows.

**Step 1.** On detecting the anomalous behavior in a zone intrusion detection system (IDS) send an “alert message to the base station” conveying the information that particular zone under the attack.

**Step 2.** Base Station (BS) checks the behavior of sensor nodes with an additional message exchange with cluster heads.

**Step 3.** Base Station (BS) will authenticate either all cluster heads under attack or the sensor nodes under a particular cluster head, which are captured or compromised. Based on this information base station inform the key distribution system (KDC) to update or revoke the keys.

**Step 4.** Key distribution system (KDC) communicates with cluster heads under its control in a zone for updating or revoking the key rings.

**Step 5.** Key distribution system (KDC) transmits the updated, “information to the base station”.

**Step 6.** Base station updates the security information about cluster heads under a particular Zone within its memory. If sensors from one zone want to communicate with other zone they first authenticate themselves from the base station by registering their session and identifiers.

V. CONCLUSIONS AND PERSPECTIVES

We have proposed decentralized technique, to renew symmetric and asymmetric keys and to establish a shared key between two authenticated nodes of the network. We proposed the use of ECC and pair based cryptography, which allows nodes to easily construct shared keys without interactions, furthermore partitioning the sensor network into zones makes the efficient management and distribution of keys. In future our study will focus on the simulation of overall networks. As a long-term perspective, we plan on testing our protocols in more realistic platforms.

REFERENCES

[1] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar,. “SPINS: Security Protocols for Sensor Networks”. Department of Electrical Engineering and Computer Sciences University of California, Berkeley Mobile Computing and Networking Rome, Italy.ACM, (2001)ISBN 1-58113-422-3/01/07

[2] Rodrigo Roman et.al.. “Key management systems for sensor networks in the context of the Internet of Things” Elsevier Journal Computers & Electrical Engineering ,Volume 37, Issue 2, March 2011, (2011).Pages 147–159

[3] L.Eschenauer.V.D.Gligor.2002."Key -management scheme for distributed sensor networks".Proceeding of the 9th ACM Conference on Computer and Communication security,(2002).,

[4] Lee and Stinson “On the Construction of Practical Key Predistribution Schemes for Distributed Sensor Networks Using Combinatorial Designs”ACM Transactions on Information and System Security (TISSEC),Volume 11 Issue 2, March 2008.

[5] Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen, and Pramod K. Varshney. “A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge”
“Proceedings of IEEE 2003 Global Communications Conference”, NY (2003)13244-1240, USA

[6] Panjna, Madria, Bhargava. “Energy and communication efficient group key management protocol for hierarchical sensor networks” Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, ISBN:97695-2553-9-01, (2006). Pages 384 - 393

[7] S. Zhu, S. Srivia, and S. Jaijodha. “efficient security mechanisms for large-scale distributed sensor networks”. In Proceedings of the 10th ACM conference on Computer and Communication Security (CCS’ 03), Washington D.C. ACM (2003) pages 62–72

[8] R. D. Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan. "Connectivity properties of secure wireless sensor networks". In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, Washington DC, USA, ACM (2014).

[9] M. Eltoweissy, M. H. Heydari, L. Morales, and I. H. Sudborough, "Combinatorial Optimization of Group Key Management", Journal of Network and Systems Management, 12(1) 2004, pp. 33–50.

[10] G. Gaubatz, J. Kaps, and B. Sunar. “Public key cryptography in sensor networks” revisited in 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004)

[11] D. J. Malan, M. Welsh, and M. D. Smith. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. In First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (IEEE SECON 2004), pp. 71–80 (2004)

[12] Seyit A, C, amtepe, B’ulent Yener. "combinatorial design of key distribution mechanisms for wireless sensor networks" IEEE/ACM Transactions on Networking (TON) Volume 15 Issue 2,Pages 346-358 April 2004

[13] D. Chakrabarti, S. Maity, and B. Roy. 2005, A Key Pre-distribution Scheme for WirelessSensor Networks: Merging Blocks in Combinatorial Design. In Information Security, pp. 89–103. LNCS 3650, (2005)

[14] Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang. “Secure Sensor Networks with Location-Based Keys” Department of Electrical and Computer Engineering University of Florida, Gainesville, FL 32611 IEEE Communications Society / WCNC (2005).

[15] B. Doyle, S. Bell, A. F. Smeaton, K. McCusker, and N. E. O’Connor.2006. Security Considerations and Key Negotiation Techniques for Power Constrained Sensor Networks. The Computer Journal, 49(4):443–453 (2006).

[16] Patrick Traynor Sencun Zhu, and Thomas La Porta. “Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks” IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 6, NO. 6, JUNE (2007).

[17] Lee and Stinson, "On the Construction of Practical Key Predistribution Schemes for Distributed Sensor Networks Using Combinatorial Designs" ACM Transactions on Information and System Security (TISSEC), Volume 11 Issue 2, March 2008.

[18] Piotr Szczecowiak et al. “NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks” 5th European Conference, EWSN 2008, Bologna, Italy, January 30-February 1, (2008).

[19] Wen Hu et.al. “secFleck: A Public Key Technology Platform for Wireless Sensor Networks” 6th European Conference, EWSN 2009, Cork, Ireland, February 11-13. Proceedings pp. 296-311 (2009).

[20] T. Kavitha and D. Sridharam.2010. “Security vulnerabilities in wireless sensor networks: a survey,” Journal of Information Assurance and Security, vol. 5, pp. 31–44, 2010

[21] K. McCusker and N. O’Connor. “Low-energy symmetric key distribution in wireless sensor networks,” Dependable and Secure Computing, IEEE Transactions on, vol. 8, no. 3, pp.363–376, May–June 2011

[22] Rodrigo Roman et al. “Key management systems for sensor networks in the context of the Internet of Things” Elsevier Journal Computers & Electrical Engineering, Volume 37, Issue 2, March 2011, Pages 147–159 (2011).

[23] Xing Zhang et al. 2011. “EDDK: Energy-Efficient Deterministic Key Management for Wireless Sensor Networks” EURASIP Journal on Wireless Communications and Networking. Article ID: 765143, DOI:10.1155/2011/765143 (2011)

[24] Leonardo B et al. “TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks” Special Issue of Computer Communications on Information and Future Communication Security Volume 34, Issue 3, 15 March 2011, Pages 485–493 (2013).

[25] Wang Wei, Wang Zhaob. “A Research of RSSI-AM Localization Algorithm Based on Data Encryption in Wireless Sensor Networks” Journal of Sensors & Transducers, Vol. 175, Issue 7, pp. 284-290 (2014).

[26] Walid Abdallah. “An Efficient and Scalable Key Management Mechanism for Wireless Sensor Networks” ICACT Transactions on Advanced Communications Technology (TACT) Vol. 3, Issue 4 (2014).

[27] Andrew Newwell et al. “Node-Capture Resilient Key establishment in Sensor Networks: Design Space and New Protocols” ACM Computing Surveys, Vol. 47, No. 2, Article 24, (2015)

[28] Lein Harn et al. “Predistribution Scheme for Establishing Group Keys in Wireless Sensor Networks” IEEE sensors Journal, VOL. 15, NO. 9. (2015).

[29] M. Eltoweissy, A. Wadaa, S. Olariu, and L. Wilson. “Group key management scheme for large-scale sensor networks” journal of Ad Hoc Networks Volume 3 Issue 5, Pages 668-688 September, 2005

[30] Seung-Hyun Seo et al. “Effective Key Management in Dynamic Wireless Sensor Networks” Information Forensics and Security, IEEE Transactions (Volume:10 , Issue: 2) pp. 371 – 383(2015).