Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No.2, May 2017 – www.caeaccess.org

Key Management Techniques in Wireless Sensor Networks

Ahmed S. Elqusy
Computer Science & Eng. Dept.,
Faculty of Electronic Eng.,
Menoufia University, Menouf 32952, Egypt

Salah E. Essa
Computer Science & Eng. Dept.,
Faculty of Electronic Eng.,
Menoufia University, Menouf 32952, Egypt

Ayman El-Sayed
Computer Science & Eng. Dept.,
Faculty of Electronic Eng.,
Menoufia University, Menouf 32952, Egypt

ABSTRACT
Wireless sensor networks are visualized in military, medicinal services applications and business, where the data at these filed is very important. Security of the information in the system relies on the cryptographic strategy and the techniques in which encryption and decryption keys are built up among the nodes. Dealing with the keys in the system incorporates node validation, key understanding and key refresh stages which represents an extra overhead on system assets. Both Symmetric and Asymmetric key methods when connected independently in WSN neglects to give a design reasonable to extensive variety of utilizations.

Keywords
Key Management, Encryption, RSA, ECC, Symmetric Encryption, Asymmetric Encryption, Hybrid Encryption.

1. INTRODUCTION
Wireless sensor networks (WSN's) are being utilized as a part of extensive variety of military and business applications. A WSN comprises of small asset limited sensor nodes and unique checking device named as base station. Sensor nodes go about as the skin, which gather the information from encompassing condition and forward to the base station, the cerebrum of the system, controls the information stream. WSN innovation is relied upon to assume critical part in not so distant future as the methods for worldwide information communication. 'Internet of things' [1] thought, proposed as of late, considers WSN as the essential component to assemble information.

The gathered information is then made all-inclusive accessible by interfacing numerous little WSNs to the Internet. In such situation, data gathered by WSN's would have risen above esteem contrasted with its past little scale application. Thusly, security of the data additionally assumes an important part. Confidentiality, Integrity and Authenticity of the information gathered are the fundamental issues in sensor network security. Remote nature of the system alongside the absence of computational capacity of sensor nodes postures many difficulties in the execution of security protocols for wireless sensor network. Key Management strategy is the important part of any system security conspire. Secured direct for information transmission in a WSN is given by key formation protocol.

The outline of key management protocol for the most part focusses on the utilization of assets like memory, power and the time of processing of the scheme, versatility against different assaults, communicating overhead and adaptability. At the framework level, the requests from key administration procedure being flexibility against node catch, forward secret, in reverse secret, node disavowal on intrusion detection and security against system level assaults. Both symmetric and asymmetric key methods utilized for PC systems neglect to fulfill these WSN particular security prerequisites. Requirements in WSN is considered as: Energy imperatives, Memory restrictions, Unreliable Communication, Unreliable Transfer, Conflicts, Latency, lastly unattended operation of systems.

Additionally there are a security issues which drives the analysts to assess any security framework. Which are: Data privacy, Data Integrity, Data freshness, Availability, Self-association, Time, synchronization, Secure Localization, Authentication, and Non-disavowal. In wireless sensor network, customary security procedures can't be connected straightforwardly. WSNs are developing quickly in numerous viewpoints, in this manner security component for WSN ought to be refreshed also. WSN works in outside condition where they are unattended, so security ought to be considered in the outline stage [2].

Security in WSN can be constructed into two types, operational and data security. Operational security implies that the system ought to have the capacity to give benefits regardless of the possibility that some of its parts come up short or progress toward becoming traded off. Data security implies that the system ought not to reveal any mystery data, in addition to it ought to ensure uprightness and legitimacy of the messages. Security is a basic necessity for WSN, the information and hub ought to be ensured against assaults like listening in, treating, DOS assault [3], and so on. When outlining a security model for WSN, all these sort of assaults ought to be considered and security ought to be characterized on various layers to guarantee high level to reliability.

Targets. Which primitives are best for a given target will be controlled by the fundamental properties of the primitives.

Key management is a center component to guarantee security in system administrations and applications in WSNs. The objective of key management is to build up the keys among the nodes in a protected and secure way. Likewise, the key management scheme must bolster node expansion and renouncement in the system. Since the nodes in a WSN have computational and control imperatives, the key management protocol for these networks must be to a great degree light-weight.

Any key management schemes needs four fundamental capacities, particularly Key examinations or key investigation,

Key task, Key era, and Key Pre-distribution. These capacities have been firmly combined with each other and it is done by a server that is centralized or the collaboration of sensor nodes in the network.

Similarly as with any system, we can assess nature of a key management conspire by assessing its properties. In [5, 4], authors distinguish nine such real properties.

Memory impression – It is clear from the specialized determination of most remote sensor nodes that their memory is altogether obliged. In this manner limiting the measure of the put away information, together with minimization of the genuine foundation code, additionally put away in the memory, is of significance. A perfect KMS from the memory impression point of view ought to just store keys with required gatherings, e.g., neighbors and additionally base station.

Processing speed – Similarly, most normally utilized microcontrollers are working on such low frequencies that playing out a computationally concentrated operation, for example, ECC point increase, may take up to seconds [7, 6] and subsequently defer whatever other calculation from performing on the nodes for a lot of time. Moreover, performing microcontroller calculations can likewise outstandingly fumes node's battery [8, 9] in this manner lessen its lifetime.

Communication overhead – The correspondence overhead is one of the major concentrations in current WSN convention plans. Truth be told, it has been indicated [10, 8, 12] that message transmission and gathering is normally the node's greatest node's vitality utilization consider. Best KMSs for WSNs ought to transmit as meager information as would be prudent, in a perfect world be preloaded with all the mutual privileged insights and no requirement for further correspondence.

Network bootstrapping – During this eliminate nodes discover their neighbors, build up keys with them, inspect the system's topology for steering purposes and perform other abutted errands. A perfect KMS ought to require no bootstrapping stage as it is the most defenseless stage in the lifetime of a sensor node. That is the time when there are altogether shared insider facts put away and an assailant could typically trade off vast bits of the system by securing these.

Network strength – This property communicates what effect would an aggressor have on the system after catching an (arrangement of) node(s). As remote sensor nodes are considered physically uncertain, the majority of their mystery information can be effectively gotten to by an assailant who catches a hub. By catching a hub with a decent KMS, just connections the hub is included in ought to end up traded off.

Connectivity – Connectivity works comparatively as in the diagram hypothesis. It depicts the capacity of two hubs (vertices) to set up a mutual mystery (an association).

More specific availability properties are:

Worldwide connectivity – Describes the likelihood of a safe way between any two nodes being set up.

Local connectivity – Describes the likelihood of any two neighboring nodes sharing a mystery.

Node availability – Describes the likelihood of any two nodes in the system sharing a mystery.

Scalability – A general system may be of self-assertive size. Adaptability communicates what amount keying information a node needs to store with respect to the measure of system. An ideal KMS is putting away a little measure of keying material that is either straightforwardly utilized as a mutual key with different hubs or the key is processed in light of this material.

Extensibility – While versatility depicts the capacity to adapt to huge number of hubs in the system, extensibility describes its capacity to add new hubs to the system and build up shared mysteries amid its lifetime. A perfect KMS ought to just store keys it may need and in this manner ought to have the capacity to set up keys with discretionary measure of new-coming hubs.

Energy – The vitality property portrays how much vitality is essential for a KMS to set up shared privileged insights. A praiseworthy KMS ought to execute as meager calculation and transmit as meager information as conceivable so as to safeguard the greatest measure of vitality on the hub.

In the reset of the paper, a taxonomy of Key management techniques will be presented in the next section. The discussion of the work and analysis of the future research trend will be proposed in section 3. Lastly, the conclusion of the work is cleared in section 4.

2. TAXONOMIES OF KEY MANAGEMENT TECHNIQUE BASED ON ENCRYPTION MECHANISMS.

As shown in Figure 1 numerous scientific categorizations for KMSs have been displayed [13, 14, 16, 13, and 5].In [13] *Network structure* – unified key methods, furthermore, appropriated key methods. The brought together key administration plans are those in light of a solitary substance in charge of key era and dispersion, regularly called the key dissemination focus (KDC). The main discovered illustrative of this class at the season of distributing was the intelligent key chain of importance plan [18], while the various considered plans fit to the conveyed key plans classification.

Probability of key sharing – probabilistic key scheme, and deterministic key scheme. The approach in view of the likelihood of key sharing separates the probabilistic key schemes and deterministic key schemes. A few recommendations may consolidate these methodologies, or utilize one for foundation of a class of keys and another for an alternate class of keys, and none of these classes would fit.

The attacker model - the authors of [14] characterize a novel characterization in view of the assailant demonstrate. They characterize four assailant models and guide the beforehand characterized key foundation conspire classes to the most grounded aggressor demonstrate they are as yet secure under.

The assailant models are characterized as takes after: Aggressor Model 1: in this model a foe can monitor the communication between nodes after the keys has been established establishment. No node catch assault is propelled amid the lifetime of the system. The mapping of master key based pre-distribution is happened in this level. Aggressor Model 2: in this model an active assaults, for example, node catch can occur after the setup of the key. Amid key setup, observing is a slim chance. Aggressor Model 3: in this model Communication checking is available directly after sending. Then again, active assaults can just show up after setup of the key.

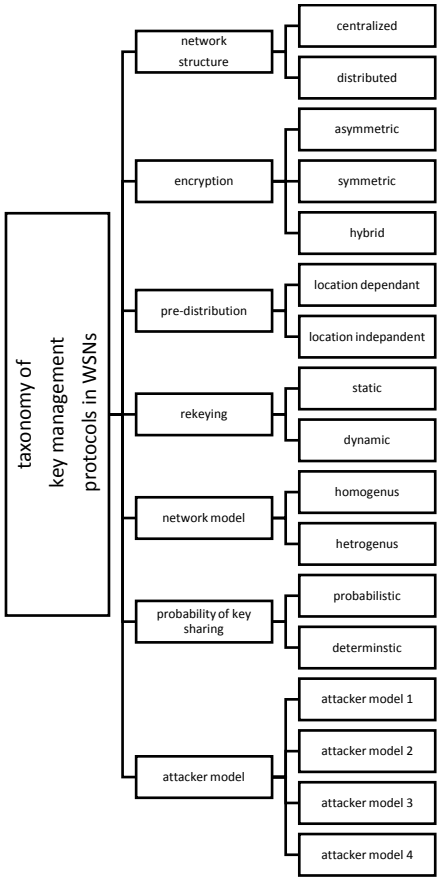

Figure 1: Classifications for KMSs

The LEAP protocol is an agent of scheme secure under this class of assailant, but it is an individual from the Master key based pre-dispersion type also. Aggressor Model 4: in this model both catching and active assaults are available ideal from the node deployment. Base station interest, i.e., the SPINS protocol, and pairwise key pre-dispersion schemes are considered consummately secure and fit to this type of model.

Depending upon key pre-distribution – It is characterized into area free key Pre-distribution and area subordinate key pre-distribution.

Depending upon Deployment – Key management Schemes can be additionally characterized into Static and element conspire in view of whether rekeying is performed after sending.

In the Static KMS conspire once the sensor node are sent in the field, they won't change regulatory keys are produced before sending. In the active KMS may change its managerial keys occasionally or on request. The significant preferred standpoint of element KMS is upgraded organize survivability and versatility. *Depending upon the network mode –,* It is ordered into homogeneous or heterogeneous scheme as to the part of system nodes in the key administration process. Homogeneous plans generally a level system model and all the sensor nodes are having same capacities, while in heterogeneous schemes are proposed for both level and hierarchical systems.

Finally, and the core of the paper which is the classification of key management baes on Encryption mechanism

The author in [16] displays an extensive overview of existing key management scheme and order them in view of the encryption enter instrument utilized as a part of the scheme. Symmetric key management schemes, Asymmetric key management schemes, and Hybrid schemes.

2.1 Based on Asymmetric Encryption.

Asymmetric Key Cryptography was presented first by W.Diffie and M. Hellman displays the principle thought of a public key cryptosystem. Because of constraints of WSNs, not all security arrangements intended for customary PC systems can be actualized straightforwardly in WSN. For quite a while, it was trusted that public key cryptography was most certainly not reasonable for WSNs since that it was required high preparing power, however through investigations of encryption calculations in view of bends was confirmed the plausibility of that strategy in WSN.[21]

2.1.1 Asymmetric Encryption Techniques.

The cryptographic algorithm RSA Is named after its creators Rivest, Shamir and Adleman [22] [23]. This technique utilizes two vast prime numbers P and Q .The quality of this algorithm depends on the complexity of finding these extensive prime numbers which is fundamental to locate the secret key while individuals in public key can be disseminated openly. Since utilizing vast prime numbers and slicing as process, it requests high operational necessities as far as assets. It will take toll on processing power memory, and the life span of the operation requests control power too. Through this strategy it is conceivable to encrypt information and to make computerized signature. It was successful to the point that today is the RSA public key algorithm utilized most on the world.

Elliptic Curve Cryptography (ECC) algorithm - In eighteenth [24] proposed a way for cryptography taking in minde elliptic curve ECC. As indicated by authors of the ECC 4, an elliptic curve is an idea of curve characterized by the accompanying condition:

$$y^2 = x^2 + ax + b$$

The effectiveness of this calculation depends on finding a discrete logarithm of an irregular element that is a part of an elliptic curve. The effectiveness of ECC cryptographic calculation with key sizes of around 160 bits is like got utilizing the RSA calculation with 1024 piece key [25]. Algorithm which has a few aspects depend on elliptic curves, counting key management, encryption and digital signature. The unadulterated content m is first spoken to as a point M, and afterward encrypted by the addition to kQ, where k is a whole number picked haphazardly, and Q is the public key. An aggressor who needs to peruse of M need to ascertain kQ. This model have been widely considered since as indicated by Amin [26] as of late the ECC has pulled in consideration as a security answer for WSN, due to the fact that the utilization of little keys and below computational overhead.

Hybrid Elliptic Curve Cryptography (HECC) algorithm - The HECC was made in 1988 by Koblitz [27] as a generality of elliptic curves. As per Batina [28] the interesting contrast amongst ECC and HECC is at normal level that for this situation comprises of various arrangements of operations. The HECC utilizes more unpredictable operations, although works with littler operands. As per Chatterjee [25] the chain of importance of operations in the HECC and ECC algorithm can be separated into three levels. The primary level is the

scalar duplication on the second level are point operations bunch/splitter and the third level, definite field operations.

Multivariate Quadratic Almost Group (MQQ) - The cryptographic algorithm exhibited above have their security in view of computationally unmanageable scientific issues: computational effectiveness of figuring the discrete logarithm and number factorization [30]. In 2008, it was presented another plan called multivariate quadratic public key near roup (MQQ) [31]. This algorithm depends on multivariate polynomial changes of almost quadratic and grouped having the accompanying properties [30, 31]. Highly parallelizable not at all like different calculations that are basically successive, the encryption acceleration is practically identical to different cryptosystems public key in view of multivariate quadratic, the decryption algorithm is same as of a symmetric block chipper, and post-Quantum Algorithm, As indicated by El-Hadely and Maia [32, 31] investigations demonstrated that the equipment MQQ can be as quick as a run of the mill symmetric block cipher, being a few requests of extent quicker than algorithm, for example, RSA, DH and ECC.

2.1.2 Asymmetric Key management schemes.

2.1.2.1 RSA-based asymmetric encryption scheme.

RSA-based asymmetric encryption scheme Watro et al. [17] depicted the TinyPK: securing sensor systems with public key innovation. They plan and execute public key-based protocol that permit verification and the agreement of key between esource compelled sensors. The TinyPK support a technique for giving validation and key trade between an outer gathering and a sensor network. TinyPK depends on the outstanding RSA cryptosystem, utilizing e ¼3 as public proponent. To achive verification, the outside gathering presents its marked public key and some content marked with its private key. Protocol operation begins when the outsider gives a challenge to the sensor network. This test comprises of two sections: The first is its own particular public key, marked by the CA (certificated authority) private key; the second is an{m aggregate object comprising of a nonce (which called a timestamp) and a message checksum, marked with the outsider's own particular private key. They additionally actualized Diffie–Hellman key exchange on the MICA2 platform. The objective of Diffie–Hellman is to give a common secret between two gatherings that can then be utilized to make a cryptographic key. They utilize Diffie–Hellman to produce a secret reasonable for use in making another or substitution TinySec key. Such a key would permit two disjoint sensor network to convey and permit the arrangement of substitution bits into a current sensor field without looking up and preload the TinySec enter being used by the field.

2.1.2.2 ECC-based asymmetric encryption system.

ECC-based asymmetric encryption system Malan et al. [19] proposes a public key framework for key dissemination in TinyOS in view of elliptic curve cryptography. Elliptic curve cryptography is executed over F2p for sensor frameworks in light of the 8-bit, 7.3828-MHz MICA2 bit. They contend that public key framework is practical for TinySec keys dissemination, even on the MICA2. They exhibit that public keys can be created inside 34 s, and that shared secret key can be circulated among nodes in a sensor network inside the same, utilizing a little more than 34KB of ROM and 1KB of SRAM. Malan et al. give a working execution of Diffie-Hellman in view of the elliptic curve discrete logarithm issue. Another sort of ECC-based public key scheme for n_authentication were proposed by Ren et al. [20]. In the event that client can effectively confirm with any subset of sensors out of an arrangement of n sensors, the n-verification succeed. Ren et al. proposed a few n-confirmation schemes in light of ECC and other cryptographic systems including the Bloom channel, the fractional message recuperation signature scheme and Merkle hash tree. The two essential plans are the certified based authentication (CAS) and the immediate storage based validation.

2.1.2.3 ID-based key agreement schemes.

This method relay on the sort algorithm of elliptic curve cryptography. Boneh and Franklin [29] proposed a completely sensible character based scheme of encryption. The inspiration of identify based encryption is to streamline the authentication based public key encryption framework. In the declaration based public key encryption framework, a client needs to confirm another client's authentication before utilizing his/her public key. Subsequently, every client requires an extensive storage and registering time to store and check each other's public keys and the relating authentication. The fundamental thought of the scheme is that a self-assertive string can act as a public key. As a result, a client can utilize any ID, for example, email, to figure a public key, instead of extricating from the authentication issued by a certification Authority (CA). An ID based encryption plan is determined by four Randomized calculations: Setup, Extract, Encrypt, and Decrypt.*ID-based key agreement scheme*,Yang et al. [50] proposed ID-based key assention conspire. This scheme comprises of the accompanying strides. Firstly, Initialization stage: In this stage, all public parameters and private keys have been calculated, and contribute the m to sensors. Then, Encrypting message stage: up on the finishing of the previous stage, a sensor system is conveyed. A node has its private key and the public parameters. Finally, Decrypting message: Plain text can be recuperated by running the Decrypt work with private key of the node. In a sensor organize without base station, just the node knows its private key. *ID-based key management scheme*, *is* another scheme has been proposed depends on the polynomials [51]. It will be shown as takes after. First, System setup: The order node or the base station needs to set up the framework to such an extent that all essential parameter output be utilized amid the WSN application's life time. Second, Algorithm development: This method comprises of the accompanying three stages: Encryption Setup, Encryption and Decryption. Encryption setup. So as to speak with group pioneers/cluster headers (gateway), the charge node needs to setup the accompanying parameters, Yang et al., show the reproduction result. It demonstrates that, for a RSA scheme, the calculation time increments with the length of keys. At a similar security level, an IBE scheme with 160Cbit key takes 6.8s, while a RSA conspire needs 29s. Moreover, the administration of keys in RSA is more unpredictable than that in IBE.

2.2 Based on Symmetric Encryption.

2.2.1 Symmetric Encryption Techniques.

2.2.1.1 Block Ciphers in WSN

A lightweight block cipher figure, with little block size and key size, is proper for WSNs, as it is energy effective and gives adequate security in Wireless Sensor Networks. We pick four block cipher as competitors and consider the diverse energy execution when connected in Wireless Sensor Networks. The chosen one block cipher are AES [33], Skipjack [34], Puffin [35] and BSPN1 [36].

Advanced Encryption Standard (AES), [33] is the most prominently sent symmetric key cipher. Despite the fact that, as we might see, the energy cost per byte of AES is high, it is by and large viewed as a protected decision when choosing ciphers for security methods.
Skipjack, [34] is promised to replace the Data Encryption Standards (DES). It is work with Wireless Sensor Networks in the TinySec method [37] because of its good use of energy. In any case, some examination has demonstrated that Skipjack has security shortcoming under specific cryptanalyses [38] [39].

Puffin, [35] currently presented smaller block cipher intended for hardware executions. Puffin can oppose differential and straight cryptanalysis and it is likewise impervious to related-key assaults and frail keys, which are two principle weaknesses of the key schedule.
Byte-wise SPN (BSPN), is a conservative block cipher we propose to use in WSNs [36], which gives direct security to the energy constrained condition. It has no obvious storage and is impervious to both the differential and direct cryptanalysis assaults [36].

2.2.1.2 Stream Ciphers in WSNs

The following stream cipher will be compared: RC4, Sosemanuk and Salsa.
RC4- which is a familiar stream cipher developing a little size (8 bit) key stream block which -exclusive or - with 8 bits of plaintext.
Sosemanuk and Salsa- which are from the eSTREAM extend, which are viewed as secure and intended for programming purposes. Despite the fact that there are likewise two other stream cipher, Rabbit and HC-128.
By comparing these techniques it showed that RC4 utilizes the least number of cycles to produce the key stream bytes for encryption.

2.2.2 Symmetric Key management schemes.

Symmetric key management scheme which is classified into three classifications, these are:

2.2.2.1 Base Station Participation Scheme.

In this technique a base station which is a trusted and secured is utilized as a judge to give an interface keys to sensor node. Every sensor node imparts a one of a unique key to a base station, which goes about as a Key distribution center (KDC). Accordingly, the plan is likewise called centralized key distribution center (KDC) approach. The sensor nodes validate themselves to the base station [75]. The scheme requires less memory and consummately controlled node replication, likewise it is versatile to node catch and conceivable to abolish key pairs. But it is not versatile and the base station turns into the objective of assaults.
The following are some of the current techniques.
Security Protocols for Sensor Networks (SPINS) [40]: SPINS is a security building hinder that is advanced for resource compelled conditions and remote communication. It depends on trusted base server. Twists depends on two secure building squares: SNEP (Secure Network Encryption Protocol) and µTESLA (the "smaller scale" adaptation of the Timed, Efficient, Streaming, and Loss-tolerant Authentication Protocol). SNEP gives the information privacy, two-party information validation, and information freshness with low overhead. While µTESLA gives validated communicate to seriously resource compelled environment.
Logical Key Hierarchy for Wireless sensor network (LKHW) [41]: it is a safe gathering communication scheme in light of coordinated dispersion and Logical Key Hierarchy (LKH) scheme, to secure the coordinated dissemination protocol. A LKH is a key tree structure within this tree leaves represent source nodes and roots represent sink node. Every leaf node keep the same keys all the way along to the sink node. It has Minimal storage, although the base station turns into the objective of assaults.

2.2.2.2 Trusted Third Node Based Scheme

In trusted third node based scheme a companion sensor node is utilized as a put stock in mediator for the creation of a mutual key between nodes. The following are some of the latest techniques.
PIKE [42]: A mechanism was proposed known as Peer Intermediaries for Key Establishment (PIKE), a key dissemination scheme depends on utilizing peer sensor nodes as put stock in middle nodes. The scheme was intended to address the absence of versatility of existing symmetric key dispersion scheme. The scheme sets up keys between any two node paying little respect to network topology or density of nodes. The scheme is admitting fewer communication overhead when contrasted with KDC approaches. The scheme is a great deal stronger than the current one. Key creation is not probabilistic. The scheme has two varieties, one is essential PIKE and at least three dimensional PIKE. Nonetheless, Intermediary node might be the objective of assault

2.2.2.3 Pre-Distribution Schemes

The key pre-distribution conspire includes three stages: key pre-distribution stage, shared-key disclosure stage and path key establishment stage.
In light of the key appropriation, key disclosure and key establishment in the pre-distribution scheme, we group these scheme into nine classes, these are:
Master Key Based Pre-Distribution Scheme:
A solitary key is preloaded into all the sensor nodes of the system. After that, each node in the system can utilize this key to encrypt and decrypt messages. This scheme incorporates negligible capacity prerequisites and evasion of complex protocol. Since single key is kept in every sensor node; no requirement for a sensor node to perform key disclosure or exchange of the key. Although, bargain of a solitary node causes the tradeoff of the whole system through the singled shared key. Broadcast Session Key negotiation protocol (BROSK) [43], the scheme depends on single master key that is pre-conveyed to nodes. Lightweight Key Management System [44], the approach requires the sensors to share a little arrangement of secret keys. These keys are stacked in every sensor before sending.
Pair-Wise Key Pre-Distribution Scheme:
In pair wise key conveyance schemes, pairwise keys are stacked to the sensor nodes before arrangement. This enables every node to speak with every one of the nodes in its communication run. This offers node to node verification, expanded strength against the node catch. In this manner limits the possibility for node replication. The disadvantage is the extra overhead required for every node to build up n-1 special key with the various nodes in the system and keep up those keys in its memory. *Random Pair-Wise Keys Scheme* [45], is a pair wise key pre-distribution conspire in which particular match insightful keys are stacked to the sensor nodes before organization.
Pure Probabilistic Key Pre-Distribution Schemes:

This technique guarantees some likelihood that any two sensor nodes can convey utilizing a pairwise key. It does not, in any case, guarantee that two nodes dependably can register a pairwise key to use for secure communication. *Random Key Pre-Distribution Scheme* [46], it permits expansion and cancellation of sensor nodes in the system after sending. It addresses the bootstrapping issue. Thus, that the system develops or supplanting falling flat and temperamental nodes. The key-dispersion prepare comprises of three stages. Firstly, key pre-dissemination. After that, shared-key disclosure. Finally way key creation stage *Q-Composite Random Key Pre-distribution Scheme* [45], In q-composite random key pre-appropriation conspire q-common keys from the key pool rather than one basic key in the essential scheme are utilized in each of the sensor node. This will build the key cover required for key-setup, in this way expanding the strength of the system against node catch. Subsequently, the scheme fortified the security under little scale assault. Be that as it may, defenselessness increments when the scheme needs to face extensive scale physical assault. *Multipath Key Reinforcement Scheme* [45], it facilitates the updates of key over numerous autonomous ways. They expected that after the setup of key different secure ways are framed in view of q basic keys shared by the nodes. It expands the security of key setup to such an extent that an assailant needs to trade off numerous more nodes to accomplish a high likelihood of bargaining any given communication. *Closest Pairwise Keys Pre-Distribution Scheme* [47, 48], the essential thought of this scheme is to pre-appropriate pairwise keys between sets of sensors. So that two sensors have a pre-disseminated pairwise key in the event that they have a high likelihood to show up in each other's RF range. *Random Key Pre-Distribution Scheme Using Node Deployment Knowledge* [49], it was presented which is utilizing node arrangement information. All the current pre-appropriation key schemes consider uniform dissemination. They considered non-uniform probability density functions (pdfs). They have demonstrated that learning would enhance arbitrary key pre-dissemination scheme [46]. *Key Pre-Distribution Using Post-deployment Knowledge* [47], it was presented which is utilizing an idea of post deployment learning of sensor nodes to enhance the pairwise enter pre-circulation in static sensor systems.

Polynomial-Based Key Pre-Distribution Schemes:

It relays on the scheme of pairwise keys pre-dispersion. Subsequently these scheme conquer a portion of the probabilistic pre-circulation schemes' impediments. These are, First, any two sensors can build up a pairwise key when there are no negotiate sensors; second, Even with a few nodes bargained, the others in the system can at present set up pairwise keys; third, A node can locate the normal keys to decide if it can set up a pairwise key and in this manner help decrease communication overhead. *Polynomial Based Pairwise Key Pre-Distribution* [52], this scheme was presented which is utilizing the idea of polynomials. It utilizes the idea of the protocol [53]. This mechanism in [53] was created for gathering key pre-conveyance. *Polynomial Pool-Based Pairwise Key Pre-Distribution* [52], it is a generic system for key pre-conveyance which is a mix of polynomial based key pre-dissemination and key pool [46, 45]. In this system a pool of haphazardly produced bivariate polynomials is utilized to set up pairwise keys between sensors. *Random Subset Assignment Key Pre-Distribution Scheme* [54, 52], A proficient instantiation of the general structure polynomial pool-based pairwise key pre-dispersion was created. An arbitrary procedure is utilized for subset task amid the setup stage. *Network Based Key Pre-Distribution* [52], it depends on the parts of the general system. Along these lines, it ensures that any two sensors can build up a pairwise key when there is no negotiate sensor. *Position Based Pair-Wise Keys Scheme*: it utilizing Bivariate Polynomials [48], which depends on polynomial-based key pre-dissemination strategy and nearest pairwise keys scheme.

Nearest Polynomials Scheme [47]: it is a blend of the normal position of sensor nodes with the irregular subset task scheme in [52] to conquer certain restrictions. *Hypercube-Based Key Pre-Distribution Scheme* [54], it is a speculation of network based key pre-conveyance scheme [52]. *Random Perturbation-Based (RPB) Scheme* [55], it depends on polynomials to create pairwise keys. The RPB does not give every node the first share but rather the perturbed share, which is the entirety of the first impart and an irritation polynomial to the restricted contamination property.

Matrix-based key pre-distribution schemes:

All conceivable connection enters in a system of size n can be act as an n × n key matrix. Little measure of data is put away to every sensor node, so that each combine of nodes can compute comparing field of the matrix, and utilizations it as the connection key.

Grid-Group Deployment Scheme [57], it was presented which is called as network gathering organization plot. Nodes are consistently sent in an extensive zone rather than haphazardly circulating keys from a huge key pool to every sensor. Secret keys are deliberately conveyed to every sensor from an organized key pool. *Robust Group-Based Key Management Scheme* [56], it was presented which is known as gathering based key administration conspire utilizing sensor arrangement learning in light of Blom' mechanism [59]. It accomplished a higher level of connectivity with the assistance of deployment learning when contrasted with the ideal scheme. *Multiple Space Key Pre-distribution Scheme* [58], A pairwise key pre-circulation mechanism was presented which depends on Blom's key pre-dissemination conspire [59] and consolidates the irregular key pre-dispersion strategy [46] with it; which offers enhanced system flexibility known as Multiple-Space Key Pre-conveyance Scheme. *Constrained Random Perturbation based pairwise establishment (CARPY) scheme* [60]:

This scheme and its variation CARPY+ was presented for WSN. In the CARPY conspire, there are two stages: the disconnected stride is performed, before sending of sensor nodes, and the on-line step-is performed for each combine of sensor nodes. The second variety is (CARPY+) Communication-Free CARPY Scheme. In the CARPY conspire, two sensor nodes speak with each other just to exchange the individual segment of G, which can be known by the enemy.

Tree-based key pre-distribution scheme:

In this scheme, senor nodes are masterminded in a tree in which every sensor node speaks with its parent node. So the key creation has done between neighboring nodes along the total tree. The plan is the fundamentally lessening of the memory cost. *ID-Based One Way Function Scheme* [61], in this scheme, a public one way hash capacity is utilized as a part of request to diminish the quantity of keys kept in the node. A remarkable ID is relegated to every sensor node and

this ID is utilized to register secret keys. *Deterministic Multiple Space Blom's Scheme* [59], it was presented to enhance the strength of the different IOSs. With a specific end goal to accomplish great strength they debilitated the availability of the system chart.

Hierarchical Key Management Scheme:
A tree of keys is worked for the progressive system, where the keys at a specific level are appropriated to the comparing class of nodes. The keys at more elevated amounts can be utilized to determine the keys at lower levels, but not the other way around. *localized Encryption and Authentication Protocol (LEAP)* [62]: underpins the creation of four sorts of keys for every sensor node an individual key imparted to the base station, a pairwise key imparted to another sensor node, a cluster key imparted to various neighboring nodes, and a group key that is shared by every one of the nodes in the system. *A Time-Based Deployment Model* [63], it was recommended that would restrict the effect of key bargain inside the time interims. The ideal opportunity for sensor nodes to set up pairwise keys each other, Test, may take longer than the time interim for an enemy to compose a node.
Combinatorial Design-based key Pre-distribution Scheme [64, 65]: a determination key and a scheme which is hybrid pre-appropriation was presented in light of Combinatorial Design hypothesis that chooses what number of and which keys to allocate to each key-chain before the sensor organize formation. The principle downsides is the complexity of its development. To conquer the downside, they proposed a Hybrid Design which joins a deterministic basic with a probabilistic expansion.
EBS-Based Key Pre-Distribution Schemes [66]:
It conspire abuses the exchange off between the quantity of authoritative keys k and the quantity of rekeying messages m. this approach turns out to be exceptionally versatile for substantial systems and empowers awesome adaptability in system administration by controlling the attitude of k and m. Huge k builds the capacity necessities at the node, while substantial m expands communication overhead for key administration. *Scalable, Hierarchical, Efficient, Location-aware, and Light-weight (SHELL) Scheme* [68], it bolsters rekeying in this way upgrades organize security and survivability against node catch. SHELL has the feature of collision-free. *Localized Combinatorial Keying (LOCK) conspire* [67] LOCK achieve confined rekeying to limit overhead. It is an enhanced version for SHELL [68]. It utilizes the key polynomials to enhance network strength to conspiracy rather than position based key task as in SHELL.

2.3 Based on Hybrid Encryption.

2.3.1 Hybrid Encryption techniques.

Symmetric key calculation has a hindrance of key appropriation [69] and asymmetric calculation require much calculation so the energy of the sensor is squandered in it [69] and it is not doable to use as power is squandered then sensor will be of no utilization Thus the calculation which joins both the calculation i.e. asymmetric and symmetric so the benefits of both the calculation can be used in it. A protocol is called s hybrid cryptosystem is utilizing numerous cipher of various sorts together, each further bolstering its best good fortune. One normal approach is to create an irregular secret key for a symmetric cipher, and after that encode this key by means of an asymmetric cipher utilizing the beneficiary's public key. The content of message is then scrambled utilizing the symmetric cipher and the secret key. Both the scrambled secret key and the encoded message are then transmit to the beneficiary. The beneficiary unscrambles the secret key in the first place, utilizing his/her own particular private key, and afterward utilizes that key to decode the message. This is fundamentally the approach utilized as a part of PGP. A portion of the hybrid algorithm like DHA+ECC [70] is portrayed in detail.

2.3.1.1 SCUR.

Tahir et al. [71] presented an inconsequential Encryption technique in view of the Rabbit stream cipher for giving privacy in WSNs. It satisfies both prerequisites of security and also energy effectiveness. The target of the SCUR is to limit cost-impact of the accompanying while at the same time keeping up required levels of security: (1) Communication overhead, in the event of conveying the encrypted packet .calculation overhead, in securing the system , to spare sensor's life time .(3) used key space.

2.3.1.2 MASA

Alzaid et al. [71] presented a security framework known as MASA (Mixture of Asymmetric and Symmetric Approaches) to give end-to-end information security for WSN. It depends on the idea of virtual geographic network wherein the whole territory is separated into littler districts called cells. Every sensor conveys two sorts of keys, asymmetric and symmetric. MASA utilizes the private key to mark a hashed occasion warning to give classification, genuineness, and information respectability. The symmetric key is utilized to validate the occasion notice inside its cell.

2.3.1.3 SecFleck

Hu et al., [74] depicted the sketch and execution of public key stage. It depends on a ware Trusted Platform Module (TPM) chip that broadens the ability of a regular node. SecFleck picks XTEA symmetric key cryptography as a result of its little RAM impression, which makes it a decent contender for small sensor device that normally have under 10 KB RAM. XTEA can be utilized as a part of a yield criticism mode to encode or discredit had examined the execution of the secFleck stage as far as calculation time, energy utilization, and monetary cost.

2.3.2 Hybrid Key management schemes.

A few research group like Huang et al., [73], and Zhangand Varadharajan, [11] presented the hybrid key establishment scheme for WSNs. The inspiration is to misuse the distinction among the base station, the cluster header and the sensor, and locate the cryptographic burden on the base station or to the sensors where their point of supply are less obliged. The establishment scheme of hybrid key lessen the huge computational cost on the sensors by setting them on the base station side.
Huang et al. [73] show a hybrid verified key establishment conspire, which depends on a mix of elliptic curve cryptography (ECC) and symmetric-key operations. The establishment protocol for hybrid key decreases the big cost elliptic curve arbitrary point scalar increases at the sensor side and replaces them with ease and proficient symmetric-key based actions.

3. DISCUSSION AND FUTURE STUDY.

The criteria for assessing WSN key administration scheme include: firstly, Computation multifaceted nature (registering overhead or preparing many-sided quality), is the quantity of unit capacity executed. Also, Communication complexity (overhead), is the amount and volume of packet sent and got

by a sensor node. After that Storage complexity (overhead), is the measure of memory units required to keep security credentials. And then, Connectivity implies the association likelihood for two nodes have the same pre-distributed key or building up a key way between them. Subsequently, Scalability implies whether a scheme bolster sensor node renouncement/expansion for substantial WSN. Finally, Security quality (resilience), implies the likelihood that a connection is bargained when a foe catches a node or the quantity of sensors required for foe to compromise the entire WSN. The productivity of security scheme: Is measured by Computation multifaceted nature, correspondence intricacy and capacity complexity, and the execution of the scheme is measured by Scalability, versatility and availability. In light of the past criteria, Symmetric-key based scheme are broadly utilized as they are moderately less calculation complexity, which are appropriate for the constrained resource attributes of the WSN. Nevertheless, the deficiencies of the symmetric key scheme are additionally self-evident. Diverse scheme may have distinctive shortcoming, for example, security quality (flexibility), and versatility and association likelihood. Then again, public key scheme have many points of interest, for example, communication overhead, storage, versatility. It can give less complex arrangement substantially more grounded security quality. Public key resolution were thought too computationally costly for remote sensor organize. The usage and reproduction results demonstrates that the ECC-based and scheme ID-based key understanding scheme have less calculation complexity. Hybrid scheme are reasonable for the bigger various leveled WSN. Hybrid scheme may have points of interest of both asymmetric key and symmetric scheme for bigger sensor network. The progressing course is the means by which to secure the WSN by joining the cryptographic methods to give the best answer for the distinctive environment.

4. CONCLUSION

Wireless Sensor Network's Key management is a basic issue that has been tended to through many proposed methods displayed in different papers. A review of these procedures is given in this paper, each of which offers Cons points and pros. A harmony between the necessities and resources of a WSN figures out which KMS ought to be utilized. A Wireless sensor network utilized as a part of a war fields needs more security than one utilized as a part of spots like strip malls; likewise, the previous can be made all the more exorbitant although the later should be as shoddy as could be expected under the circumstances. Choices with respect to the key management scheme to be utilized must be founded on these necessities for productivity. The investigation of key management in WSN still has bottomless research openings later on. As electrical frameworks wind up plainly littler, all the more intense, and utilize less vitality, the security restrictions will turn out to be more unpredictable. With respect to now, key administration frameworks are an exchange off of execution and security to low overhead in memory use and message transmissions. Key administration frameworks sole reason for existing is to supply secure communication in WSN without delivering much overhead. More methods ought to be produced to make proficient utilization of sensor nodes' restricted resources. More noteworthy accentuation ought to be given to the security in KMS, especially as a larger part of sensor node sending is in threatening situations where giving solid security elements is an unquestionable requirement. Despite the fact that getting much consideration as of late, there are numerous issues to be tended to in WSNs, for example, finding the traded off nodes in a system, making great utilization of sending information, making nodes carefully designed without much overhead, diminishing the bootstrapping time required for the system, and so forth. Relish research ought to particularly look for procedures for traded off node disclosure and effective techniques to renounce bargained nodes. Various lives can be spared in wars with the information gathered by sensors, however Wireless sensor networks sooner rather than later will offer many shocks for out of this world to be utilized as a part of day by day family unit matters like locking entryways and turning off gadgets, or controlling activity in high-volume regions. Sensors introduced in huge shopping centers and malls can control individuals to their required items effortlessly while those in clinics can screen persistent condition and those in backwoods can give prompt learning about heartbreaking risks like out of control fire. These points of interest are just a little division of what Wireless sensor networks could conceivably offer when sent all the more regularly. Future reviews can end up being valuable in a more extensive assortment of situations.

5. REFERENCES

[1] Atzori, L., Iera, A., & Morabito, G. 2010. The internet of things: A survey. Computer networks, 54(15), 2787-2805.

[2] Walters, J. P., Liang, Z., Shi, W., & Chaudhary, V. 2007. Wireless sensor network security: A survey. Security in distributed, grid, mobile, and pervasive computing, 1, 367.

[3] Deng, J., Han, R., & Mishra, S. 2003. Enhancing base station security in wireless sensor networks. Technical Report CU-CS-951-03, Department of Computer Science, University of Colorado.

[4] JURNEČKA, F. (2013). Key management schemes in wireless sensor network simulations (Doctoral dissertation, Masarykova univerzita, Fakulta informatiky).

[5] Roman, R., Lopez, J., Alcaraz, C., & Chen, H. H. (2011, March). SenseKey--Simplifying the Selection of Key Management Schemes for Sensor Networks. In Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on (pp. 789-794). IEEE.

[6] Oliveira, L. B., Aranha, D. F., Gouvêa, C. P., Scott, M., Câmara, D. F., López, J., & Dahab, R. (2011). TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. Computer Communications, 34(3), 485-493.

[7] Szczechowiak, P., Oliveira, L. B., Scott, M., Collier, M., & Dahab, R. (2008). NanoECC: Testing the limits of elliptic curve cryptography in sensor networks. In Wireless sensor networks (pp. 305-320). Springer Berlin Heidelberg.

[8] Shnayder, V., Hempstead, M., Chen, B. R., Allen, G. W., & Welsh, M. (2004, November). Simulating the power consumption of large-scale sensor network applications. In Proceedings of the 2nd international conference on Embedded networked sensor systems (pp. 188-200). ACM.

[9] Perla, E., Catháin, A. Ó., Carbajo, R. S., Huggard, M., & Mc Goldrick, C. (2008, October). PowerTOSSIM z: realistic energy modelling for wireless sensor network environments. In Proceedings of the 3nd ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks (pp. 35-42). ACM.

[10] Pottie, G. J., & Kaiser, W. J. (2000). Wireless integrated network sensors. Communications of the ACM, 43(5), 51-58.

[11] Zhang J, Varadharajan V. (2008).Group-based Wireless Sensor Network Security Scheme. In: The fourth international conference on wireless and mobile communica- tions (ICWMC).

[12] Anastasi, G., Conti, M., Di Francesco, M., & Passarella, A. (2009). Energy conservation in wireless sensor networks: A survey. Ad hoc networks, 7(3), 537-568.

[13] Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks.

[14] Lee, H., Kim, Y. H., Lee, D. H., & Lim, J. (2007). Classification of key management schemes for wireless sensor networks. In Advances in Web and Network Technologies, and Information Management (pp. 664-673). Springer Berlin Heidelberg.

[15] Simplício, M. A., Barreto, P. S., Margi, C. B., & Carvalho, T. C. (2010). A survey on key management mechanisms for distributed wireless sensor networks. Computer networks, 54(15), 2591-2612.

[16] Zhang, J., & Varadharajan, V. (2010). Wireless sensor network key management survey and taxonomy. Journal of Network and Computer Applications, 33(2), 63-75.

[17] Watro, R., Kong, D., Cuti, S. F., Gardiner, C., Lynn, C., & Kruus, P. (2004, October). TinyPK: securing sensor networks with public key technology. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (pp. 59-64). ACM.

[18] Di Pietro, R., Mancini, L. V., Law, Y. W., Etalle, S., & Havinga, P. (2003, October). LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks. In Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on (pp. 397-406). IEEE.

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

[20] Ren, K., Yu, S., Lou, W., & Zhang, Y. (2009). Multi-user broadcast authentication in wireless sensor networks. IEEE Transactions on Vehicular Technology, 58(8), 4554-4564.

[21] SenthilKumar, U. S. M. N., & Senthilkumaran, U. (2016). Review of asymmetric key cryptography in wireless sensor networks. International Journal of Engineering and Technology, 8(2), 859-862.

[22] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[23] Shamir, A. (1984, August). Identity-based cryptosystems and signature schemes. In Workshop on the Theory and Application of Cryptographic Techniques (pp. 47-53). Springer Berlin Heidelberg.

[24] Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of computation, 48(177), 203-209.

[25] Chatterjee, K., De, A., & Gupta, D. (2011). Software Implementation of Curve based Cryptography for Constrained Devices. International Journal of Computer Applications, 24(5), 18-23.

[26] Amin, F., Jahangir, A. H., & Rasifard, H. (2008). Analysis of public-key cryptography for wireless sensor networks security. World Academy of Science, Engineering and Technology, 41, 529-534.

[27] Koblitz, N. (1990, February). A family of Jacobians suitable for discrete log cryptosystems. In Proceedings on Advances in cryptology (pp. 94-99). Springer-Verlag New York, Inc..

[28] Batina, L., Mentens, N., Preneel, B., & Verbauwhede, I. (2006, May). Flexible hardware architectures for curve-based cryptography. In Circuits and Systems, 2006. ISCAS 2006. Proceedings. 2006 IEEE International Symposium on (pp. 4-pp). IEEE.

[29] Boneh, D., & Franklin, M. (2001, August). Identity-based encryption from the Weil pairing. In Annual International Cryptology Conference (pp. 213-229). Springer Berlin Heidelberg.

[30] Gligoroski, D., Markovski, S., & Knapskog, S. J. (2008). A public key block cipher based on multivariate quadratic quasigroups. arXiv preprint arXiv:0808.0247.

[31] Maia, R. J. M. (2010). Analysis of the viability of the implementation of the algorithms post-Quantico besides in quadratics multivariate almost-groups in platforms of boundary processes (doctorate, University of São Paulo).

[32] El-Hadedy, M., Gligoroski, D., & Knapskog, S. J. (2008, December). High performance implementation of a public key block cipher-mqq, for fpga platforms. In Reconfigurable Computing and FPGAs, 2008. ReConFig'08. International Conference on (pp. 427-432). IEEE.

[33] Pub, N. F. 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/NIST, November 26, 2001. Available from the NIST website.

[34] SkipJack and KEA Algorithm Specifications. National Institute of Standards and Technology, version 2, may 1998.

[35] Cheng, H., Heys, H. M., & Wang, C. (2008, September). Puffin: A novel compact block cipher targeted to embedded digital systems. In Digital System Design Architectures, Methods and Tools, 2008. DSD'08. 11th EUROMICRO Conference on (pp. 383-390). IEEE.

[36] Heys, H. M., & Tavares, S. E. (1996). Substitution-permutation networks resistant to differential and linear cryptanalysis. Journal of cryptology, 9(1), 1-19.

[37] Karlof, C., Sastry, N., & Wagner, D. (2004, November). TinySec: a link layer security architecture for wireless sensor networks. In Proceedings of the 2nd international conference on Embedded networked sensor systems (pp. 162-175). ACM.

[38] Granboulan, L. (2001, April). Flaws in differential cryptanalysis of Skipjack. In International Workshop on Fast Software Encryption (pp. 328-335). Springer Berlin Heidelberg.

[39] Knudsen, L., Robshaw, M., & Wagner, D. (1999). Truncated differentials and Skipjack. In Advances in Cryptology—CRYPTO'99 (pp. 790-790). Springer Berlin/Heidelberg.

[40] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. Wireless networks, 8(5), 521-534.

[41] Di Pietro, R., Mancini, L. V., Law, Y. W., Etalle, S., & Havinga, P. (2003, October). LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks. In Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on (pp. 397-406). IEEE.

[42] Chan, H., & Perrig, A. (2005, March). PIKE: Peer intermediaries for key establishment in sensor networks. In INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE (Vol. 1, pp. 524-535). IEEE.

[43] Lai, B., Kim, S., & Verbauwhede, I. (2002, December). Scalable session key construction protocol for wireless sensor networks. In IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES) (p. 7).

[44] Dutertre, B., Cheung, S., & Levy, J. (2004). Lightweight key management in wireless sensor networks by leveraging initial trust. Technical Report SRI-SDL-04-02, SRI International.

[45] Chan, H., Perrig, A., & Song, D. (2003, May). Random key predistribution schemes for sensor networks. In Security and Privacy, 2003. Proceedings. 2003 Symposium on (pp. 197-213). IEEE.

[46] Chan, H., Perrig, A., & Song, D. (2003, May). Random key predistribution schemes for sensor networks. In Security and Privacy, 2003. Proceedings. 2003 Symposium on (pp. 197-213). IEEE.

[47] Liu, D., & Ning, P. (2005). Improving key predistribution with deployment knowledge in static sensor networks. ACM Transactions on Sensor Networks (TOSN), 1(2), 204-239.

[48] Liu, D., & Ning, P. (2003, October). Location-based pairwise key establishments for static sensor networks. In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (pp. 72-82). ACM.

[49] Du, W., Deng, J., Han, Y. S., Chen, S., & Varshney, P. K. (2004, March). A key management scheme for wireless sensor networks using deployment knowledge. In INFOCOM 2004. Twenty-third AnnualJoint conference of the IEEE computer and communications societies (Vol. 1). IEEE.

[50] Geng, Y. A. N. G., Rong, C. M., Veigner, C., Wang, J. T., & Cheng, H. B. (2006). Identity-based key agreement and encryption for wireless sensor networks. The Journal of China Universities of Posts and Telecommunications, 13(4), 54-60.

[51] Zhang J,VaradharajanV. (2008, July).Group-based Wireless Sensor Network Security Scheme. In: The fourth international conference on wireless and mobile communications (ICWMC2008).

[52] Liu, D., & Ning, P. (2003, October). Location-based pairwise key establishments for static sensor networks. In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (pp. 72-82). ACM.

[53] Blundo, C., De Santis, A., Herzberg, A., Kutten, S., Vaccaro, U., & Yung, M. (1992, August). Perfectly-secure key distribution for dynamic conferences. In Annual International Cryptology Conference (pp. 471-486). Springer Berlin Heidelberg.

[54] Liu, D., Ning, P., & Li, R. (2005). Establishing pairwise keys in distributed sensor networks. ACM Transactions on Information and System Security (TISSEC), 8(1), 41-77.

[55] Zhang, W., Tran, M., Zhu, S., & Cao, G. (2007, September). A random perturbation-based scheme for pairwise key establishment in sensor networks. In Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing (pp. 90-99). ACM.

[56] Yu, Z., & Guan, Y. (2005, March). A robust group-based key management scheme for wireless sensor networks. In Wireless Communications and Networking Conference, 2005 IEEE (Vol. 4, pp. 1915-1920). IEEE.

[57] Huang, D., Mehta, M., Medhi, D., & Harn, L. (2004, October). Location-aware key management scheme for wireless sensor networks. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (pp. 29-42). ACM.

[58] Du, W., Deng, J., Han, Y. S., Varshney, P. K., Katz, J., & Khalili, A. (2005). A pairwise key pre-distribution scheme for wireless sensor networks. ACM Transactions on Information and System Security (TISSEC), 8(2), 228-258.

[59] Blom, R. (1984).Theory and Application of Cryptographic Techniques. Proceedings of the Euro crypt 84 Workshop on Advances in Cryptology, Springer, Berlin, pp. 335–8.

[60] Yu, C. M., Lu, C. S., & Kuo, S. Y. (2009, June). A simple non-interactive pairwise key establishment scheme in sensor networks. In Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on (pp. 1-9). IEEE.

[61] Lee, J., & Stinson, D. R. (2004, August). Deterministic key predistribution schemes for distributed sensor networks. In International Workshop on Selected Areas in Cryptography (pp. 294-307). Springer Berlin Heidelberg.

[62] Zhu, S., Setia, S., & Jajodia, S. (2006). LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. ACM Transactions on Sensor Networks (TOSN), 2(4), 500-528.

[63] Jang, J., Kwon, T., & Song, J. (2007, May). A time-based key management protocol for wireless sensor networks. In International Conference on Information Security Practice and Experience (pp. 314-328). Springer Berlin Heidelberg.

[64] Çamtepe, S. A., & Yener, B. (2007). Combinatorial design of key distribution mechanisms for wireless sensor networks. IEEE/ACM Transactions on networking, 15(2), 346-358.

[65] Camtepe, S. A., & Yener, B. (2004, September). Combinatorial design of key distribution mechanisms for wireless sensor networks. In European Symposium on Research in Computer Security (pp. 293-308). Springer Berlin Heidelberg.

[66] Eltoweissy, M., Heydari, M. H., Morales, L., & Sudborough, I. H. (2004). Combinatorial optimization of group key management. Journal of Network and Systems Management, 12(1), 33-50.

[67] Eltoweissy, M., Moharrum, M., & Mukkamala, R. (2006). Dynamic key management in sensor networks. IEEE Communications magazine, 44(4), 122-130.

[68] Younis, M. F., Ghumman, K., & Eltoweissy, M. (2006). Location-aware combinatorial key management scheme for clustered sensor networks. IEEE transactions on parallel and distributed systems, 17(8), 865-882.

[69] Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks.

[70] Beg, M. R., & Ahmad, S. (2012). Energy Efficient PKI Secure Key management Technique in Wireless Sensor Network Using DHA & ECC. International Journal of Ad Hoc, Sensor & Ubiquitous Computing, 3(1), 21.

[71] Alzaid, H., & Alfaraj, M. (2008, November). MASA: End-to-End Data Security in Sensor Networks Using a Mix of Asymmetric and Symmetric Approaches. In New Technologies, Mobility and Security, 2008. NTMS'08. (pp. 1-5). IEEE.

[72] Zhang, J., & Varadharajan, V. (2010). Wireless sensor network key management survey and taxonomy. Journal of Network and Computer Applications, 33(2), 63-75.

[73] Huang, Qiang, et al. "Fast authenticated key establishment protocols for self-organizing sensor networks." Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications. ACM, 2003.

[74] Wen, H., Nirupama B., Chun T. C., Sanjay J., Andrew T., Van N. T. (2009).Design and evaluation of a hybrid sensor network for cane toad monitoring. ACM Transactions on Sensor Networks (TOSN).

[75] Bala, S., Sharma, G., & Verma, A. K. (2013). Classification of symmetric key management schemes for wireless sensor networks. International Journal of Security and Its Applications, 7(2), 117-138.