Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7– No. 24, December 2018 – www.caeaccess.org

A Research Study on different Key Management Strategies for Large Scale WSNs

Premakumar M. N.
Research Scholar, Department Electronics & Communication, Dr. AIT, Bengaluru, Karnataka, India

Ramesh S, Phd
Professor, Department of Electronics & Communication Engineering, Dr. AIT, Bengaluru, Karnataka, India

ABSTRACT
A wireless sensor network technology is immensely utilizing in multiple fields, for example; physical environment monitoring, surveillance systems, object tracking systems, robotic systems and many more. Usually, wireless sensor nodes are deployed in remote or hostile environments, and such sensors are vulnerable to compromise different attacks; therefore, a suitable and efficient key management scheme is essential at this point. Recently, different key management approaches are proposed by different researchers to address security challenges, especially for WSNs. Since key management is a core scheme to ensure security for network resources along with solving the problem of key generation, distribution, and secret key management. Hence, in this investigational study have to provide a detailed study on reliable key management techniques which are playing a vital role in large-scale WSNs. This study classifying the key management scheme into Asymmetric based and Symmetric based key management schemes and highlighting their functionalities by evaluating performance parameters. In the beginning, the study defines a workflow of the key management system followed by life cycle. Additionally, have briefly discussing popular key-management algorithmic approaches their applications and limitations.

Keywords
Elliptic Curve Cryptosystem (ECC), Encryption, Key Management, Security, Wireless sensor networks

1. INTRODUCTION
Due to the continued acceptance of wireless sensor network applications, sensor nodes are largely deploying in several applicatory areas, like smart home, intelligent transportations, fire detection in forest area, a harmful gas explosion in chemical industries and many more [1]. However, every WSN configured with several tiny sensors which are characterised by computational and sensing capabilities, limited storage and power constraints, in the meantime, the base station is a highly trustworthy and powerful main device which will act like middleware for network user and sensor devices. Since sensor networks have the nature of the wireless channel, it is frequently subject to different threats (e.g., snooping attack, compromised node and intercept, etc.). Once the sensor node is subjected by the attacker, the all information stored in that sensor is disclosed, the whole network will be in danger of extinction [2-3]. Hence WSN security is the most important to stop information leakage. To ensure high security, key management scheme is the significant aspect which will be a safeguard for any WSNs. Key management (KM) is the process where setting up the security keys between the sensors nodes and administer the secret keys for cryptography. The process involves key generation, distribution, storage, protection, replacement and employ of said keys with another security system make into robust and large cryptosystem allows selective limitation for certain-keys. Key management is one of the prominent challenging tasks of cryptosystem as it deals with multiple security liabilities further than encryption. Additionally, for multicast clustering, security is a big challenge, because all sensors in the clusters have the capability to receive the multicast information. The solution is the key management scheme, in which specific secrete keys are distributed for each sensor. In this order, the encryption method uses a specific key for each sensor by which information can only be retrieved and read by that specific group member. The most common example for key management scheme is public-key infrastructure, which is utilized in the transport layer and sockets layer security.

However, several researchers survey on key management scheme for WSNs [4]– [9]. From the case study, have concluded that key management is prominent for WSNs security, where different key distribution and key management schemes are utilized for many WSNs applications [10]. Additionally, a public key cryptography method is used for WSNs security, i.e. elliptic curve cryptographic method [11]. In [12] authors introduced a Low-cost Ssecret Data Sharing (LSDS) scheme for WSN, which offers a security fundamental to create secure communication link via interchanging of secret keys between the adjacent nodes using non-cryptography methods and increases the secret-key establishment with authentication. Nevertheless, since key exchange takes place between the sensors, and it consumes more amount of energy. Furthermore, the authentication among the adjacent nodes also requires a large set of data exchange, in the results it not suitable for WSNs.

De Amorim et al. [13], proposed a secret message sharing mechanism using secure data aggregation method. In this framework, sensors are responsible to splits the message packets and exchange and transfer them between multiple paths to stop the tampering attack and eavesdropping attack, also present a multi-path secure aggregation scheme which uses secret key exchange which creates distributed environment to ensures security for compromised sensor nodes. Therefore, such key management schemes are not effectively suitable for more energy consumption. In the meantime, in this approach, the network must share multiple messages to establish a secret key, which utilizes maximum energy [14]. Thus, in this survey study, have comparing existing studies towards key management scheme which is classified based on attack types [15], public keys and key pre-distribution method [16], hierarchical and dynamic key-management schemes are organized based on various key-encryption strategies [17], [18] and finally comparing solution methods based on cluster-based WSN architecture [19]. However, from the past years to till, there are several reviews have presented where key management schemes are categorized and discussed thoroughly. By considering the overall importance of key management scheme for WSN architecture, a comprehensive survey study is required at this stage.

The remaining part of the study is structured as; section-II discusses workflow of key management scheme with architecture followed by key management lifecycle. Section-III illustrates about recent research towards different key management schemes. Additionally, different security key management algorithmic approaches are discussing in section-IV. The section-V highlights the open research challenges found from the prior studies as well as conclusion of the study.

2. ABOUT KEY MANAGEMENT SCHEME

A proper key management scheme deals with the key generation, sharing, storage, usage and replacement of cryptographic key in a security system. In every cryptographic system, a proper key management scheme contains effective cryptography for security. Therefore, in this section have to discuss the detail flow process of key management scheme with architecture is shown in the figure-1. Also knows about how data encryption will perform over the network.

2.1 Key Management System Work Flow

.

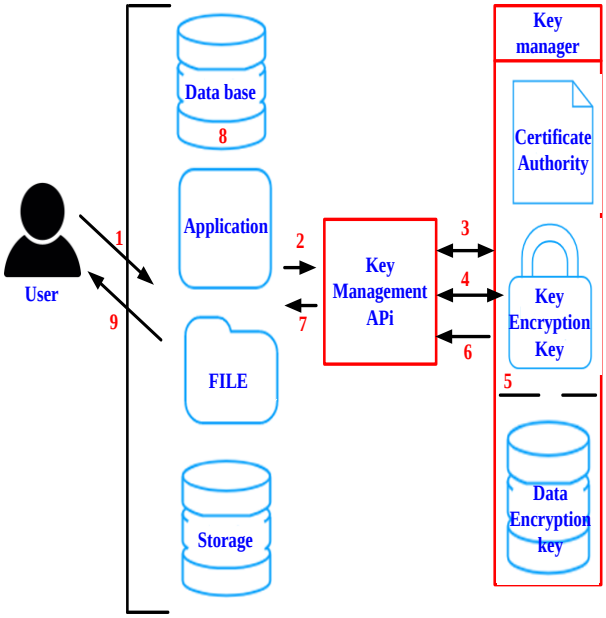

Fig 1: Generic flow process of the key management system

Now, let see how key management system works and how an authorized person can access the encrypted information; the steps are as follows.

i. Initially, a user sends a request for accessing encrypted data.

ii. The DB, file system or storage device forwards a data encryption key retrieval request to the key manager API (i.e., Client).

iii. Then, the key manager and client check each other's certificates;

a. Key manager verifies the client certificate.

b. One more certificate verification has been done by the key manager against certificate authority for authentication purpose.

c. One the client certificate verification has been done, and then the key manager forwards a verified certificate to the client for the authentication and final acceptance.

iv. After the certificate acceptance, the transport layer security protocol establishes communication among the key manager and client API.

v. Then the key manager will decrypt the requested data-encryption-key with key-encryption-key.

vi. The key manager forwards a data encryption key to the client on an encrypted transport layer security session.

vii. In the end, the key manager forwards an encrypted data key to the DB, file system, application or storage, and encrypted data key is a temporary store in the cache memory.

viii. In the result, the end user can get the plaintext information from the DB, file system, application or storage.

2.2 Key Management Life-Cycle

The key management process is the set of operations essential to create, manage, control and secure the use of encryption keys. The generic view of the key management lifecycle includes multiple phases which are briefly describing in this section with the pictorial diagram (i.e., figure -2 generic key management lifecycle).

The typical key management lifecycle is being compromised with eight major phases, and each phase represents a particular process.

- **Creation: -** The key generation is the initial phase in the key management lifecycle. The creation of key must be performed in a secure manner, and also include the requirement to match with needs for separation of tasks. In most of the cases, the generated key will be symmetric or shared key.

Additionally, during the selection of the appropriate key, the key manager endeavour to select an appropriate encryption algorithm which has been subjected to examine the review. Once the key is generated and has been properly reviewed, later it can be suitable to secure the data by encrypting with public key cryptography (i.e., asymmetric key pair).

In the case where the shared key must be distributed to the other systems, specifically through the networks, the system is recommended to follow this practice. From the viewpoint of key separation tasks, an organization may contain one team and control the key generation box, but block them access to cryptosystem itself, need them to instead of symmetric key encryption with the public shared key before offering it to the team deployment.

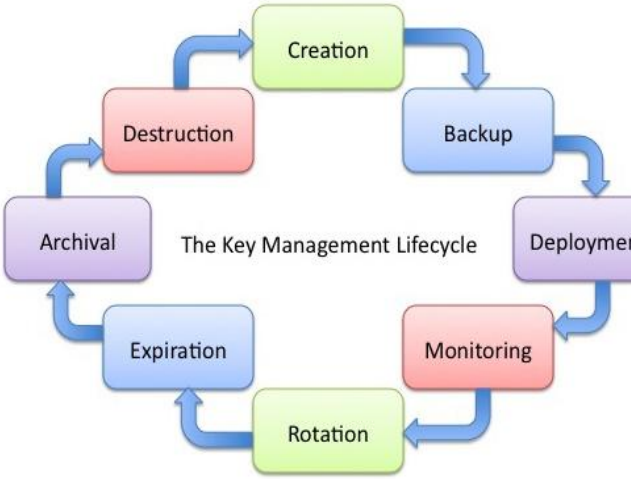

Fig 2: Generic Key management Lifecycle

- **Backup: -** During key establishment process, the first system generates new secret-key which is essentially considered for backup. The backup could be in terms of storing data into the external media, for example, CD, DVD, or USB drive, etc. or it can be in existing traditional backup solution example; local/networked. In the traditional backup scenario, it is majorly recommended that secondary asymmetric key-pair is utilized to secure the symmetric key. In the deployment of the key pair, it is recommended the generated public key is exploited to decode the shared-key, and later it becomes essential for the part of symmetric key-pair be secured and exploited for system recovery process.

One more consideration in the backup task is to utilize the same recovery strategy for any business planning process. The secret key is stored in and retrieved from the location which can be utilized within the specified time requirements by authorized business owners.

- **Deployment: -** As already stated, a new symmetric-key can be encrypted and further utilized as public-key in node deployment. The deployment phased provides a separation task in the network where the key-management process is not followed by a single system. A particular system may require for key distribution task to ensure that a single node/system may not generate, deploy the key, and decrypt the information without authorization.

The intention of the key deployment task is to generate the new secret key into the cryptosystem. The advantage of this phase is no charge for eliminating of existing or old key from the repository. Specifically, this phase is recommended for new key deployment, and it is validated for a specified time period which guarantees that can successfully deploy new secret key with data loss.

- **Monitoring: -** The monitoring phase happens parallel during the whole lifecycle process. Basically, there are three core aspects to symbolize the monitoring.
- During the unauthorized accessing, monitoring task performs an essential role to ensure the un-approved key-management process can have positive consequences for your confidential data and your system.
- In every cryptographic system monitoring phase responsible for validating the processor intensive, it means; the user system may be under process, where encryption services may happen, and there may be chances of data corruption or data redundancy.
- Key monitoring during production phase considers as an essential task to guarantee the key has been generated and deployed successfully. If deployed is corrupted, the system may offer catastrophic results. In the same manner, if there is fault occur in a cryptosystem, then the output results may also interrupt the network service, which may lead negative impact on business.
- **Rotation: -** The key rotation process is associated with the key deployment phase. The goal is to generate a new encryption key for active process and convert all encrypted and stored data into a new key. This process consumes more time. However, consider that all existing tasks of the life cycle have followed, and the key rotation task can be focused on the data conversion process, and less focus on new key generation for further encryption.

The alert message: indicate no elimination of old key from the system until the system can be confirmed that there is no data in the storage with the old key. This task may fail due to some diligence, i.e., performing the manual or individual query for the old key which may result in service expire or data loss.

Bearing alert message, the life cycle flow process (figure-2) demonstrate that the old key (i.e., first generated key) overlaps the new key lifecycle. At this stage, can notice that both key rotation and key expiration tasks are overlapping among the two keys. Also note that the rotation task is managed as a separate task from the key deployment since of its unique features, individual key installation into cryptosystem.

One of the advantages of this phase can minimize some amount of load during key rotation.

- **Expiration: -** The selection of encryption key primarily takes into an account of the time period by which data may be validated. To increase key strength, there is a best practice where keys can be replaced in a pre-specified time period and evaluate the key lifespan duration. If there is minimum key lifespan, then it is preferred as shorter key for data protection with high sensitivity rate.

In the key-management process, expiration task indicates the initial phase for key deprecation period. The rotation phase should be completed earlier to expiration, with all encrypted data the old key has been converted into a new key. The intention is to have replaced key within the system production before the expiration period. It means that the expiration task considers for planning for key conversion.

- **Archival: -** Archived key-management requires integrity and confidentiality protection. Where confidentiality needs archived encryption key and integrity requires achieved integrity key. In this

archived key may be public or private key pairs or symmetric keys.

Generally, the key archive should verify the signature key, secret authentication key, and public authentication key, the encrypted key used for key wrapping and domain parameters. Another thing is that in this phase, archive storage has some conditional policies; here system uses the master key for key-derivation and derived key. Those keys validate the encrypted archived data by decrypting archived encryption key.

However, if a user wants to destroy a key into the cryptosystem, but that key is associated with some amount of data. Then KM derived a key from the master key and transport as a private key to the user. Based on the determination, the stored data may be encrypted with archived storage key.

There are some couple of points for archiving keys;

- Index and document the key and its associated encrypted data in a way that, there must be data recovery with the archived key. A key document also associated with specific time in which the key was utilized to help for searching the appropriate key in recovery task.
- Ensure that, a replica of the archived key should be secured. As mentioned in the key creation and key deployment phase, it can be helpful for symmetric-key encryption with half of asymmetric key-pair.

It is noting that some cryptographic methods automatically document the expired keys in a secure manner and may not be utilized for further phase, destruction. It can be concluded that encrypted keys will never proceed from archival phase to destruction because the chance of such modification, and some data loss, may balance the risk of divulging the archived

- **Destruction: -** The life cycle of KM ends with the destruction of the key. In this phase, the process should follow security policy for key deletion in order to ensure that successfully destroyed.

3. RESEARCH TOWARDS KEY MANAGEMENT SCHEME OVER WSNS

In this section have to discuss about prior research studies towards different key management mechanisms in wireless sensor networks.Security is the major concern for wireless sensor network design. Also, less power consumption and storage in sensor networks leads to a highly sensitive environment to offer security. Hence, in this regards M.Anzani et al. [20] addressed a method of sharing the secret-keys among the sensor nodes as named as the key management problem. To ensure secure link establishment between the adjacent nodes, those nodes must share a common secret key.

Zhang et al. [21] have classified the different key management based on encryption methods; namely symmetric encryption, asymmetric encryption, and hybrid approach. Authors described and discussed key management solution strategies on these three classifications. In [22] Xiaobing et al. explored a concept of dynamic key management scheme for WSNs. The study classified the KM methods in two core categories; i) distributed and ii) centralized. A KM approach is dynamic when the pair-wise shared keys are reinvigorated periodically. Xiangqian et al. [23], studied on vulnerabilities and security problems over WSNs. Also, they summarized the advantages and limitations of existing key management techniques in WSNs. In [24], the authors introduced the different KM strategies on WSNs with classifying 8 classes; network-wide KM scheme, full-pair-wise KM schemes, probabilistic approach, polynomial-based, matrix-based KM approach, combinatorial design, and Key deployment knowledge-based approach. In the probabilistic approach, the authors speak about various deployments by 3 proposals; RoK [25], RGM [26] & ZoRoK [27]. In [28], Chi-Yuan et al. explored a survey study on the classification of key management schemes based on location-awareness of sensor nodes. More survey studies are proposed in [28]-[31].

More recently, the author of [32] surveys key management schemes in WSNs for securing group communication. In this work, the author considers only key management schemes dedicated to group communication security and classifies them in centralized, contributory, and hybrid. In [33]-[35], authors address self-healing within key management solutions.

Key management (KM) scheme is self-healing when sensor nodes are able to recover lost session keys without the intermediary of a key distribution center. The meaning of self-healing differs when we have multiple deployments of sensor nodes. In MPWSNs, the goal of self-healing is to diminish (up to zero if possible) the impact of node compromising attacks.

Table 1: Survey of different key management (KM) scheme

Survey papers	Aim and scope
[21, 23, 24, 28, 29, 30, 31]	A case study on different key management methods for designing secure WSNs.
[33, 34, 35]	Surveys of self-healing key management schemes.
[22]	The objective to introduce a dynamic key management solution for wireless networks, where encryption keys are refreshed or modified dynamically or on demand.
[32]	Improve the security level inside the WSNs with the help of key management solution.

M.Dasdari et al. [36] investigated significant challenges and issues on key management scheme for wireless body area networks also provide a comprehensive literature review of them. Additionally, the study classified the key management techniques as non-biometric and biometric categories and described their characteristics in detail. Finally, they highlighted their significant features and drawbacks.

In recent years, there is continuous growth in the development of WSN security technology which is majorly focusing on key management scheme and authentication policies. Such a research study carried out by D.Qin et al. [37], where the author introduced a lightweight key management scheme as well as an authentication mechanism to solve the malicious nodes problem happening during network establishment. Also, provide a solution strategy with high level security with minimum cost. The study outcomes represent that the proposed technique is well suitable for WSN security with minimum power consumption, especially for mobile sensors.

Another research study focused on security analysis on cluster-based sensor networks and proposed a session key deployment mechanism for them [38]. The objective of the study was to eliminate the vulnerabilities of existing methods and improvise the security at a high level. For security aspects, authors adopted an elliptic curve Diffei Hellman key exchange mechanism and hash-chain approach. Also, the author adopted an asymmetric

key approach, which is considered more efficient for low cost computation as compared to another similar approach in state-of-the-art key establishment scheme.

Similarly, in [39] author introduced a disjoint key-establishment scheme for WSNs, where every sensor node is preloaded with matrix format. After the key deployment, row and column indices are interchanged between the adjacent nodes and generated index values are utilized for the computation of key on each sensor node. The system performance has been verified in NS-2 simulation and analyzed by robin logic theory. From the simulation outcomes, the authors showed the efficiency of the proposed key establishment scheme and compared with prior methods in terms of storage and communication cost reduction.

From the past decades to present, it has been seen continuous research progress in WSN deployment and their security system. Several research proposals have been explored key management schemes for WSNs. In [40] A.Laould et al. proposed a self managing master key mechanism for future WSNs. The contribution of this study is to extend the previous work and make more flexible because the addition of new sensors and sensor mobility are considered into account. From this experimental study author demonstrated that the proposed KM scheme guarantees to take the less time, resource allocation with high level security assurance.

Ghasemzadeh et al. [41] have presented an analytical approach to broadcast authentication protocol. Initially, authors analyzed broadcast authentication protocol and showed that base station authenticated messages creates a route for serious DoS attacks. In the end, the study offers simulation results and conclude that the adversary node can flood the network with false information. Also, the adversary node can force the network to resend the false information's. This may lead to extreme power exhaust nodes memory that is a serious challenge for WSNs. Additionally, they introduced a security model based on hash function and resolved the security related issues in the broadcast authentication process.

However, there are different trust-based security routing protocols were proposed and designed by several authors that are considered as essential for the performance enhancement in wireless networks. But most of them have disadvantages, for example, limited energy constrained, limited security against malicious attacks owing to non-secure wireless communication channels. To defeat such security challenges, J.Kaur et al. [42] have illustrated a trust-based key management routing scheme that creates a secure and trustworthy communication route based on past and present node to node interactions. The established secure route is then remodified by isolating compromised nodes. In the last, the experimental results showed that proposed trustworthy key management scheme is more effective for discovering a secure route and increase the data delivery rate.

In [43] Messai et al. introduced another lightweight key management scheme for WSNs which is named as sequence based key management method. In this approach, pre-process is sensor nodes distribution and applied a recursive formulation for numerical computation. This process insured that establishment of keys to every node with an adjacent node after its deployment with numerical computation. The analysis of proposed method showed the system performance efficiency and author confirmed that proposed key management scheme is more reliable in terms of secure route establishment for secure communication and also provides high resilience against adversary nodes as compared to existing methods.

The biggest challenge in almost all WSN application is the security constraint. Due to the lack of security services (i.e., authentication, confidentiality, and integrity, etc) many security attacks will happen in the network. Such services are regularly provided by implementing cryptographic techniques where sensor nodes require a set of secrete keys. Therefore, by considering such type of challenge for future WSNs, W.Abdallah et al. [44] have investigated model approach of efficient and scalable key-distribution and key management scheme. In this approach, the author utilized different encryption keys to ensure security for group communications. The proposed key distribution and management scheme is performed using elliptic-curve shared key encryption and Differ Hellman method that provided key distribution and key exchange among the sensor nodes at different levels of network structure. Additionally, the re-keying scheme is also performed using a public key encryption method. This approach is highly efficient than existing methods in terms of reducing processing power during the accomplishment of key exchange. Also, this technique optimizes the memory size and improves the scalability of large size sensor networks.

In the study of Mansour et al. [45] have illustrated a key management protocols intended to revoke and renewal the keys using the elliptic curve and symmetric key cryptography method. For comparative analysis authors implemented all proposed protocols on simulation area using telosB motes and talked about their performances. In [46] Ezhilarasie et al. provided a survey study on most relevant key-management mechanisms by evaluating their performance parameters such as efficiency, scalability, key distribution and connectivity, and authentication, etc.

To maintain a balance on network security performance and network computation, in [47] Cui et al. dynamic key distribution scheme are proposed. Also introduced four different keys, is derived from the primary master key and enhanced the key management protocol using Differ Hellman algorithmic approach. In the last, the performance analysis of proposed key management protocols was analyzed through the system computational efficiency, memory requirement, and communication cost.

The several research studies are mainly concentrated on heterogeneous wireless sensor network deployment for the incorporation of different sensor nodes with various capabilities. Generally, a WSN contains either minimum sensor nodes with high power or large-scale sensors with less power constrained. Depending upon the application requirement and security demands, the varieties of key distribution and management scheme are available for heterogeneous networks. For example [48] introduced a hierarchical key-management approach for heterogeneous WSNs. In this study, the author adopted a symmetric key encryption algorithm with low cost functions with modular theory. For performance analysis, they showed the proposed scheme is more secure and reliable for heterogeneous WSNs.

In [49] Shnaikat and Alqudah discussed different key-management mechanisms, theoretically criticized them and explored an idea in the way for expected challenges for the future WSN deployment. Another survey study has been carried out by Selva and Baburaj [50], where the author reviewed on different key-management techniques their advantages and limitations. Also, provide a research direction towards implementation of key management scheme for WSN applications. One more survey study [51] illustrated the

significance characteristics and role of key management scheme for WSN security. Authors classified the different key-management schemes based on cryptography method. Additionally, key pre-distribution and key renewal mechanisms have been analyzed, and their advantages and drawbacks also summarized.

Shaila and Manjula [52], have explored a key distribution concept for mobile device authentication in WSNs. The major intention was to provide an efficient and secure communication protocol for WSNs. The author introduced a key-management protocol algorithm for double key encryption with time validation which is entirely based on the time period which validates the secure secret-key. A mobile device has been utilized to deploy and exchange the keys between the two communication channels. In the last simulation results were analyzed based on comparisons with existing studies.

From the case study, can say that there are several dynamic key-management mechanisms have been introduced for wireless sensor networks. In [53] He and Meer have explored the significant role of dynamic key-management in WSN environment, as well as defined the fundamental evaluation metrics. In this survey study, the author classified different dynamic key management schemes based on their evolution metrics. Also explored the possible research directions for future network deployment. One more survey study of key management scheme was proposed for multi phase WSNs [54]. In dynamic WSN environment, new sensors can be added or replaced on the network by post deployment process which ensures network connectivity and covers the network region in the area of interest. This network configuration is named as multiphase WSN. In this study author reviewed, classified and analyzed the performance of prior key management techniques and highlighted the advantages and limitations of those schemes.

In the study of [55], the author illustrated the scope and need of key-management scheme as well as discussed, their impact on the model of key-management solutions. This paper discussed the compliances of key-management and classified them based on respective domains such as physical security, logical security, and personal security. Meanwhile, in [56] Bhaskar and Pais introduced a new key-management algorithm for Hierarchical WSNs using Chinese remainder theory. The experimental results provided high performance with respect to minimum computation, communication time and storage cost for each sensor node, also this scheme is scalable and very effective to defeat the different attacks.

The next section overviewed on existing key-management algorithms and provided a comparative analysis of them based on their performance metrics, e.g. resilience, scalability, communication, computation and storage cost, etc.

4. EXISTING ALGORITHMIC APPROACHES

In this section have briefly discussed about popular key-management schemes their applications and limitations. There are different key-management algorithms discussed in the survey paper for WSNS [57]. The below table-2 represents the comparative analysis of exiting algorithms with respect to performance metrics (i.e., resilience, processing rate, communication range, and storage capacity.

Table 2: Comparative analysis of different key-management algorithms

Method	Theory	Resilience	Processing Rate	Communication Range	Storage capacity
Probabilistic method [58]	Random graph theory	Medium	Medium	Medium	High
Q Composite method [59]	Random graph theory	Good	Medium	High	High
Polynomial method [60]	T-degree polynomial theory	Good	High	Medium	High
Matrix method [61]	Symmetric theory	Good	Medium	Medium	High
Node deployment info-based method [62]	Random graph theory	Excellent	Medium	Medium	medium

From the above table can identify that all algorithmic approaches have their own limitations. Some of them required high computing power but some provide efficient connectivity [60], or they have sufficient storage and communication range [59], [61]. Therefore, from the case study of existing algorithms, an improved or extended key-management algorithm is needed for real time WSN environment. Therefore, in [56] authors introduced a key-management algorithm for Hierarchical WSNs using Chinese remainder theory.

In [63] Ayman classified the different key-management algorithms into two core categories, i.e. 1) Asymmetric encryption based and 2) Symmetric encryption-based algorithm. Watro et al. [64] proposed asymmetric encryption-based RSA algorithm which depicted the small PK secure sensor model with public key generation. The generated public key protocol allows for verification and creates an agreement bound between neighboring sensors. Additionally, Differ Hellman key distribution mechanism also adopted and provided general secret key sharing among the sensors.An ECC asymmetric encryption algorithm has been introduced by Malan et al. [65]. In this study, they introduced a public key novel approach for key dissemination for TinyOS and executed on F2p at WSNs with the 7.39MHz MICA-2 bit. Another ECC based asymmetric algorithm is introduced for multiple authentications [66]. One more sort of ECC based algorithms is proposed by Boneh [67] which is completely based on an encryption scheme. The intension of ID based encryption scheme is to offer authentication based public-key encryption model, where the user wants to confirm another user's authentication before the utilization f his or her secret keys. The core idea behind this approach is that a self-assertive object can behave like a public key. In [68] Yang et al. explored an identity based key declaration method which comprises the associated strides. Another ID based key-management scheme [69] has been explored using polynomial theory. In this context, a proposed framework comprises three phases; i) system setup, ii) Encryption and iii) Decryption. From the performance, analysis

author concludes that proposed algorithmic based framework can apply for WSN real time applications.

Meanwhile, the symmetric key-management scheme is categorized into three groups [63]; 1) Base-station participation technique, where base-station is utilized as an examiner to provide an edge key for sensor nodes. Each node communicates with a single unique key to the base-station, which further treated as a key distribution point. This mechanism takes very less memory and versatile to sensor catch. 2) Trusted 3rd node-based scheme; is utilized as inter mediator for generation of mutual keys for adjacent nodes. In paper [70], the author proposed a scheme of intermediary's key management scheme where peer sensor nodes are used symmetric key approach to set-up the keys between adjacent nodes which pays quite an attention to the network topology.

A master-key based pre-distribution management scheme [71], pre-distribution of pairwise key, random key pre-distribution management scheme [72], probabilistic key distribution scheme [73], closest pair-wise pre-key distribution method [74] and many more key pre-distribution schemes are proposed by several researchers by which all scheme is mainly utilized to achieve high security for WSN applications. Furthermore, pre-distribution key management scheme is grouped as polynomial based [73]-[75], matrix based [76], tree based [77] and hierarchical key pre-distribution schemes [78]-[81].

The essential criteria's for developing and designing a WSN key management scheme involve; i) evaluation multifaceted nature (i.e., pre-preparing multi-sided quality), is the amount of model capacity executed. As well as communication complexity, where the number of packet transmission and received by sensor nodes. Another factor is storage complexity and connectivity. To resolve such requirements, there is essential to select or design a proper key-management scheme to offer multiple functionalities for future WSN applications. The following table-3 highlights the classification of Asymmetric and symmetric key management schemes with their functionalities.

Table 3: Classification of Asymmetric and Symmetric KM Schemes

Asymmetric KM algorithms	Functionality	Symmetric KM algorithms	Functionality
RSA based encryption algorithm	Provide validation and key trade among sensor nodes	Centralized key-distribution approach	Require less memory, conceivable to remove key pairs, offer secure communication
ECC based encryption algorithm	Circulate secrete key between the nodes, n-validation, and storage-based verification	Trusted 3rd node based key management algorithm	Increases the network density, offer strong security
ID based encryption algorithm	Streamline authentication, extensive storage, calculate the processing time with key length validation	Key Pre-distribution approach	Offers node to node validation, Less chances of node replication, solve bootstrapping problems
-	-	Hierarchical KM approach	Enhance the network lifetime

5. CONCLUSION

In this investigational research study, have providing an overview in the state of art key management scheme for WSNs security. There are various forms of open research issues about reviewing majority of the recent work towards secure key management techniques as following:

- Existing approaches of key management techniques uses complex cryptographic techniques which is bit unpractical to be executed over resource-constrained sensors.
- There is no denying the fact that there has been lot of approaches towards key management techniques; however, they don't emphasize on securing the generating key after key distribution operation is completed.
- Similarly, studies towards key distribution mechanism doesn't emphasized on the fact that if attack scenario changes there is a need of second layer of security/encryption.
- Very less amount of research approaches are found towards the direction of the non-cryptographic based approach which is more feasible to be operational within a sensor node.
- Existing studies are not much focused upon proving any relationship between security demands of distribution and management phases in WSN

As a security view point, a dynamic and efficient key-management scheme is gaining more attention to the engineers and researchers. In this paper, we discussed existing KM approaches and highlighted their techniques and security performances of each scheme. Finally, in the last section, the study summarized and validated the KM algorithm performance based on evaluation metrics. In conclusion, it is not feasible to find an effective KM approach can provide 100% security for future WSNs. The ultimate goal of this research study is to motivate the engineers and researchers to develop and introduce a potential key management scheme for large scale wireless sensor networks.

6. REFERENCES

[1] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002) 'A survey on sensor networks,' in IEEE Communications Magazine, Vol. 40, No. 8, pp.102–114.

[2] Zhou, Y., Fang, Y. and Zhang, Y. (2008) 'Securing wireless sensor networks: a survey', in IEEE Communications Surveys & Tutorials, Vol. 10, No. 3, pp.6–28.

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

[4] X. He, M. Niedermeier, H. De Meer, Dynamic key management in wireless sensor networks: A survey, Journal of network and computer applications 36 (2) (2013) 611–622.

[5] X. Chen, K. Makki, K. Yen, N. Pissinou, Sensor network security: a survey, IEEE Communications Surveys & Tutorials 11 (2) (2009) 52 73.

[6] M. A. Simpl´ıcio Jr, P. S. Barreto, C. B. Margi, T. C. Carvalho, A survey on key management mechanisms for distributed wireless sensor networks, Computer Networks 54 (15) (2010) 2591–2612.

[7] T. Rams, P. Pacyna, A survey of group key distribution schemes with self-healing property, IEEE Communications Surveys & Tutorials 15 (2) (2013) 820–842.

[8] B. Tian, S. Han, S. Parvin, J. Hu, S. Das, Self-healing key distribution schemes for wireless networks: A survey, The Computer Journal 54 (4) (2011) 549–569.

[9] Q. Wang, Practicality analysis of the self-healing group key distribution schemes for resource-constricted wireless sensor networks, in: Third International Conference on Communications and Mobile Computing (CMC), IEEE, 2011, pp. 37–40.

[10] Katiyar, V., Chand, N. and Soni, S. (2010) 'Clustering algorithms for heterogeneous wireless sensor networks: a survey', International Journal of Applied Engineering Research, Vol. 1, No. 2, pp.273–274, Dindigul

[11] Bos, J.W., Kaihara, M.E., Kleinjung, T., Lenstra, A.K. and Montgomery, P.L. (2009) 'On the security of 1024-bit RSA and 160-bit elliptic curve cryptography', IACR Cryptology ePrint Archive, p.389.

[12] Bertier, M., Mostefaoui, A. and Tredan, G. (2010) 'Low-cost secret-sharing in sensor networks', in 2010 IEEE 12th International Symposium on High-Assurance Systems Engineering (HASE), pp.1–9.

[13] Claveirole, T., de Amorim, M.D., Abdalla, M. and Viniotis, Y. (2008) 'Securing wireless sensor networks against aggregator compromises', in IEEE Communications Magazine, Vol. 46, No. 4, pp.134–141.

[14] 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.

[15] 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.

[16] 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.

[17] Zhang, Y., Li, X., Liu, J., Yang, J. and Cui, B. (2012a) 'A secure hierarchical key management scheme in wireless sensor networks', International Journal of Distributed Sensor Networks, pp.1–8.

[18] Zhang, Y., Li, X., Yang, J., Liu, Y., Xiong, N. and Vasilakos, A.V. (2012b) 'A real-time dynamic key management for hierarchical wireless multimedia sensor networks', Multimedia Tools and Applications, Vol. 67, No. 1, pp.97–117.

[19] 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)m 865-882.

[20] Anzani, Mohaddese, Hamid Haj Seyyed Javadi, and Vahid Modirir. "Key-management scheme for wireless sensor networks based on merging blocks of symmetric design." Wireless Networks 24, no. 8 (2018): 2867-2879.

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

[22] X. He, M. Niedermeier, H. De Meer, Dynamic key management in wireless sensor networks: A survey, Journal of network and computer applications 36 (2) (2013) 611–622.

[23] X. Chen, K. Makki, K. Yen, N. Pissinou, Sensor network security: a survey, IEEE Communications Surveys & Tutorials 11 (2) (2009) 52–73.

[24] M. A. Simpl´ıcio Jr, P. S. Barreto, C. B. Margi, T. C. Carvalho, A survey on key management mechanisms for distributed wireless sensor networks, Computer Networks 54 (15) (2010) 2591–2612.

[25] C. Castelluccia, A. Spognardi, Rok: A robust key pre-distribution protocol for multi-phase wireless sensor networks, in: Third International Conference on Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007., IEEE, 2007, pp. 351–360

[26] M. Ergun, A. Levi, E. Savas, A resilient key predistribution scheme for multiphase wireless sensor networks, in: 24th International Symposium on Computer and Information Sciences, ISCIS 2009., IEEE, 2009, pp. 375–380.

[27] K. Kalkan, S. Yilmaz, O. Z. Yilmaz, A. Levi, A highly resilient and zone-based key predistribution protocol for multiphase wireless sensor networks, in: Proceedings of the 5th ACM symposium on QoS and security for wireless and mobile networks, ACM, 2009, pp. 29–36.

[28] C.-Y. Chen, H.-C. Chao, A survey of key distribution in wireless sensor networks, Security and Communication Networks 7 (12) (2014) 2495– 2508.

[29] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, M. Galloway, (a survey of key management schemes in wireless sensor networks, Computer Communications 30 (1112) (2007) 2314 – 2341, special issue on security on wireless ad hoc and sensor networks. doi:http://dx.doi.org/10.1016/j.comcom.2007.04.009

[30] A. K. Das, A survey on analytic studies of key distribution mechanisms in wireless sensor networks, Journal of Information Assurance and Security 5 (5) (2010) 526–553.

[31] A. S. Reegan, E. Baburaj, Key management schemes in wireless sensor networks: A survey, in: 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT), IEEE, 2013, pp. 813-820.

[32] O. Cheikhrouhou, Secure group communication in wireless sensor networks: A survey, Journal of Network and Computer Applicationsdoi: http://dx.doi.org/10.1016/j.jnca.2015.10.011.

[33] T. Rams, P. Pacyna, A survey of group key distribution schemes with self-healing property, IEEE Communications Surveys & Tutorials 15 (2) (2013) 820–842.

[34] B. Tian, S. Han, S. Parvin, J. Hu, S. Das, Self-healing key distribution schemes for wireless networks: A survey, The Computer Journal 54 (4) (2011) 549–569.

[35] Q. Wang, Practicality analysis of the self-healing group key distribution schemes for resource-constricted wireless sensor networks, in: Third International Conference on Communications and Mobile Computing (CMC), IEEE, 2011, pp. 37–40.

[36] Masdari, Mohammad, Safiyyeh Ahmadzadeh, and Moazam Bidaki. "Key management in wireless Body Area Network: Challenges and issues." Journal of Network and Computer Applications 91 (2017): 36-51.

[37] Qin, Danyang, Shuang Jia, Songxiang Yang, Erfu Wang, and Qun Ding. "A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks." Journal of Sensors 2016 (2016).

[38] Kim, Jiye, Jongho Moon, Jaewook Jung, and Dongho Won. "Security analysis and improvements of session key establishment for clustered sensor networks." Journal of Sensors 2016 (2016).

[39] Ghafoor, AtaUllah, Muhammad Sher, Muhammad Imran, and Imran Baig. "Disjoint Key Establishment Protocol for Wireless Sensor and Actor Networks." Journal of Sensors 2016 (2016).

[40] Laouid, Abdelkader, Abdelnasser Dahmani, Hani Ragab Hassen, Ahcène Bounceur, Reinhardt Euler, Farid Lalem, and Abdelkamel Tari. "A self-managing volatile key scheme for wireless sensor networks." Journal of Ambient Intelligence and Humanized Computing (2018): 1-16.

[41] Ghasemzadeh, Hamzeh, Ali Payandeh, and Mohammad Reza Aref. "Key management system for WSNs based on hash functions and elliptic curve cryptography." arXiv preprint arXiv:1711.08570 (2017).

[42] Kaur, Jugminder, Sandeep S. Gill, and Balwinder S. Dhaliwal. "Secure trust based key management routing framework for wireless sensor networks." Journal of Engineering 2016 (2016).

[43] Messai, Mohamed-Lamine, Hamida Seba, and Makhlouf Aliouat. "A lightweight key management scheme for wireless sensor networks." The Journal of Supercomputing 71, no. 12 (2015): 4400-4422.

[44] Abdallah, Walid, Noureddine Boudriga, Daehee Kim, and Sunshin An. "An efficient and scalable key management mechanism for wireless sensor networks." In Advanced Communication Technology (ICACT), 2015 17th International Conference on, pp. 480-493. IEEE, 2015.

[45] Mansour, Ismail, Gérard Chalhoub, and Pascal Lafourcade. "Key management in wireless sensor networks." Journal of sensor and actuator networks 4, no. 3 (2015): 251-273.

[46] Ezhilarasie, R., A. Umamakeswari, and T. Renugadevi. "Key management schemes in wireless sensor networks: a survey." International Journal of Advanced Intelligence Paradigms 7, no. 3-4 (2015): 222-239.

[47] Cui, Baojiang, Ziyue Wang, Bing Zhao, Xiaobing Liang, and Yuemin Ding. "Enhanced key management protocols for wireless sensor networks." Mobile Information Systems 2015 (2015).

[48] Chen, Chien-Ming, Xinying Zheng, and Tsu-Yang Wu. "A complete hierarchical key management scheme for heterogeneous wireless sensor networks." The Scientific World Journal 2014 (2014).

[49] W. Abdallah, N. Boudriga, D. Kim and S. An, "An efficient and scalable key management mechanism for Wireless Sensor Networks," *2015 17th International Conference on Advanced Communication Technology (ICACT)*, Seoul, 2015, pp. 480-493.

[50] Reegan, A. Selva, and E. Baburaj. "Key management schemes in wireless sensor networks: a survey." In Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on, pp. 813-820. IEEE, 2013.

[51] Sharmila, R., P. C. Gopi, and V. Vijayalakshmi. "A Survey Of Key Management Schemes In Wireless Sensor Networks." International journal of computer & organization trends 3, no. 9 (2003).

[52] Shaila, K., S. H. Manjula, K. R. Venugopal, and Lalit M. Patnaik. "Mobile node authentication using a key distribution scheme in wireless sensor networks." International Journal of Ad Hoc and Ubiquitous Computing 12, no. 1 (2013): 34-45.

[53] He, Xiaobing, Michael Niedermeier, and Hermann De Meer. "Dynamic key management in wireless sensor networks: A survey." Journal of Network and Computer Applications 36, no. 2 (2013): 611-622.

[54] Messai, Mohamed-Lamine, and Hamida Seba. "A survey of key management schemes in multi-phase wireless sensor networks." Computer Networks 105 (2016): 60-74.

[55] Paek, Kwang-Jin, Jongwan Kim, Chong-Sun Hwang, and Ui-Sung Song. "An energy-efficient key management protocol for large-scale wireless sensor networks." In *Multimedia and Ubiquitous Engineering, 2007. MUE'07. International Conference on*, pp. 201-206. IEEE, 2007.

[56] Bhaskar, Pranave Kumar, and Alwyn R. Pais. "A Chinese remainder theorem based key management algorithm for the hierarchical wireless sensor network." In International Conference on Distributed Computing and Internet Technology, pp. 311-317. Springer, Cham, 2015.

[57] Akyildiz, F., Su, W., Sankarasubramaniam, Y., Cyirci, E.: Wireless Sensor Networks: A Survey. Computer Networks 38(4), 393–422 (2002)

[58] Eschenauer, L., Gligor, V.: A Key-Management Scheme for Distributed Sensor Networks. In: Proc. of ACM CCS (2002)

[59] Chan, H., Perrig, A., Song, D.: Random Key Pre distribution Schemes for Sensor Networks. In: IEEE Symposium on Research in Security and Privacy (2003)

[60] Liu, D., Ning, P.: Establishing Pairwise Keys in Distributed Sensor Networks. In: 10th ACM CCS, Washington D.C (2003)

[61] Blom, R.: An optimal class of symmetric key generation systems. In: Beth, T., Cot, N., Ingemarsson, I. (eds.) EUROCRYPT 1984. LNCS, vol. 209, pp. 335–338. Springer, Heidelberg (1985)

[62] Du, W., Deng, J., Han, Y., Chen, S., Varshney, P.: A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge. In: IEEE Infocom (2004).

[63] S, Ahmed & E, Salah & El-Sayed, Ayman. (2017). A Key Management Techniques in Wireless Sensor Networks. Communications on Applied Electronics. 7. 8-18. 10.5120/cae2017652600.

[64] 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.

[65] 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.

[66] 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.

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

[68] 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.

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

[70] 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.

[71] 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.

[72] 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.

[73] 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.

[74] 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.

[75] 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.

[76] 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.

[77] 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.

[78] 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.

[79] 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.

[80] 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.

[81] 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.