Journal of Theoretical and Applied Information Technology
30th November 2019. Vol.97. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SURVEY OF KEY DISTRIBUTION IN THE CONTEXT OF INTERNET OF THINGS

[1] ORIEB ABUALGHANAM, [2] MOHAMMAD QATAWNEH, [3] WESAM ALMOBAIDEEN

[1] Ph.D candidate. The University of Jordan, Department of Computer Science, Jordan
[2]Professor. The University of Jordan, Department of Computer Science, Jordan
[3]Professor. The University of Jordan, Department of Computer Science, Jordan
[3]Professor. Rochester Institute of Technology, UAE
E-mail: [1] oriebabualghanam@yahoo.com, [2] mohd.qat@ju.edu.jo, [3] almobaideen@inf.ju.edu.jo, [3]wxacad@rit.edu

ABSTRACT

In recent years, with massive advancements in the Internet, the world is witnessing an evolution of smart environments facilitated by the deployment of the Internet of Things (IoT). IoT refers to a system of interrelated users and objects that are interconnected and have a significant impact on our lives. However, one of the most important challenges facing the ubiquitous adoption of IoT technology is security. In this regard, key distribution refers to the core process of setting up secure connection through a communication channel. This paper surveys the status of research until 2019 related to key distribution schemes in the context of IoT. Moreover, the classification of a key distribution is presented. In this study, we have conducted comparisons between different key distribution schemes in terms of memory storage, communication costs, and computation costs. Additionally, we propose a new taxonomy of symmetric key distribution while proposing a hybrid hierarchical architecture for the key distribution in the context of fog computing. Relevant observations and inferred recommendations are also given as one of the contribution of this paper. On the basis of these recommendations, a hybrid key distribution architecture is proposed to better enable new technologies of cloud and fog computing over IoT.

Keywords: *BIBD, Encryption, Hierarchical Architecture, Internet of Things, Key Distribution, Security,*

1. INTRODUCTION

IoT may comprise of the following components: things, net- works, data, and services [1, 2]. Things may be any object such as sensors [3, 4], humans, cameras, PCs, phones, etc. that are interconnected through a network. These things are expected to grow dramatically wherein by 2020, the estimated number of connected devices are likely to exceed 21 billion, and cites are expected to be smart. Therefore, the IoT has emerged as a promising technology to start the design of smart environments such as smart home, smart campus, smart building, etc. and other human activities such as route planning, transportation traffic decision, healthcare monitoring, and many others [5].

The IoT devices may generate, process and exchange a tremendous amount of data that can be leveraged in safety, efficiency and infotainment applications. The communication between IoT devices needs to be monitored and managed by the cloud service provider (CSP). The CSP needs to be sure that no IoT node with malicious intent can thrive in such a network.

Because the traffic generated by a malicious node can cause a degradation in the performance of other sensors. Therefore, secure communication is highly required in IoT in order to guarantee a secure exchange of data through its environment due to the fact that the majority part of IoT devices are resource constrained devices with limited storage or memory size, battery lifetime, communication bandwidth, and performance computing [6]. These limitations should be taken into consideration in the design of a key distribution protocol [7, 8].

The security issues in IoT are not fully explored and thus there is still a need for more studies in order to provide secure communication between any two parties. The process of key distribution is considered as a major part of secure

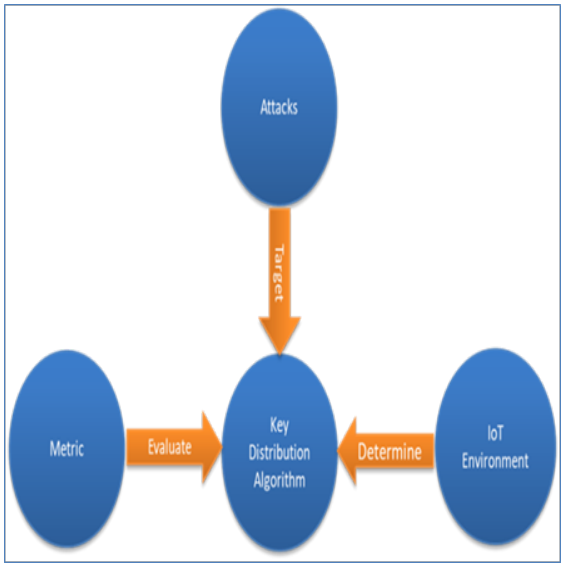
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

communication which provides a secure shared link between two or more nodes. The majority part of IoT devices are resource constrained devices with limited memory size, battery lifetime, communication bandwidth, and performance computing. These limitations should be taken into consideration in the design of key distribution protocol [9].

To appreciate the importance of the role of key distribution in the overall security systems in IoT, as well as which particular key distribution mechanism is suitable to achieve the goals of security, we begin our discussion by exploring the concept of key distribution schemes from three viewpoints: that of the metrics, attacks and that of IoT environment as shown in Figure 1. The metrics used to evaluate the key distribution algorithms in terms of efficiency and performance. IoT environment nature should be taken into consideration in the selection of a suitable and applicable scheme [10]. Finally, the survey reviews the key distribution schemes based on what type of attacks it prevents.

Figure 1: Different Aspects of Key Distribution Schemes

Table 1 provides a summary of related papers that have discussed the key distribution, highlighting the contribution of each paper ordered by the year of publication. Our survey paper differs from the other survey papers on many points as follows:



1. Surveying the key distribution schemes in the IoT environment not for a specific environment such as WSN, traditional network, Ad hoc and MANET.
2. Reviewing the recent proposals for different key distribution schemes which are up to 2019.
3. Proposing a new guideline for a suitable symmetric key style in different scenarios based on the size of the network, the communication style and the network type.
4. Providing a recent survey paper only about the key distribution as in [11] but for updated proposals.
5. Classifying the key distribution in the context of IoT into three categories based on the ways of the encryption technique: symmetric, asymmetric and hybrid. Then dividing the symmetric techniques into three subcategories: probabilistic, deterministic and other schemes.
6. Discussing the performance of several symmetric, asymmetric and hybrid key distribution schemes.
7. Comparing the most popular asymmetric key distribution schemes.
8. Classifying the three types of key distribution according to different parameters.
9. Proposing key distribution schemes for the Cloud Fog IoT architecture.

The remainder of this paper is organized as follows: Section 2 discusseses the key distribution techniques in IoT context. Section 3 presents comparisons and recommendations and in section 4 the proposed Architecture is presented. Finally, the conclusion is presented in section 5.

Table.1 Summary of Survey Papers in Key Distribution Schemes

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Ref	Year(Journal)	Environment	Period of time for reviewed papers	Summary of Contribution
[11]	2003 (ACM)	Traditional Network	1976-2002	1. Classifying the proposed key management protocols for a secured group communication into three main classes: centralized, decentralized and distributed. 2. Comparing between different group key management protocols in terms of memory storage cost of leaving and joining process. Also, in terms of backward and forward secrecy.
[12]	2004 (Springer)	Sensor Network	1982-2003	1. Reviewing several symmetric key distribution schemes and key establishment techniques for sensor networks. 2. Providing a more detailed discussion of their work on random key distribution in particular.
[13]	2006 (IEEE)	AD HOC network	1976-2005	1. Presenting a survey for ad hoc networks of key management, and shows their applicability for network-layer security. 2. Classifying the key management scheme into contributory and distributive and comparing them in terms of their characteristics.
[14]	2008 (IEEE)	WSN	1946-2007	1. Presenting a comprehensive survey of WSN security issues. 2. Reviewing different key management schemes to provide the security requirements and comparing them in terms of memory storage and local compromise probabilities.
[15]	2010 (Elsevier)	WSN	1985-2008	1. Classifying the proposed key management scheme in WSN based on the encryption techniques: into three categories symmetric, asymmetric and hybrid. 2. Classifying the symmetric and asymmetric schemes into eight and three subcategories, respectively, based on the key establishment mechanism. 3. Comparing between different schemes in terms of their performance and efficiency.
[16]	2011 (Wiley)	WSN	1978-2010	1. Classifying the proposed key distribution schemes into location independent and location-dependent key distribution schemes. 2. Comparing between different Location independent and Location dependent key distribution schemes in terms of communication, computation and storage overhead.
[17]	2014 (arXiv.org)	WSN	1976-2011	1. Presenting a survey of symmetric key distribution schemes for WSNs. 2. Proposing a new approach of key distribution using the piggy bank method.
[18]	2014 (IEEE)	Not specific	2001-2013	1. Presenting a survey for the traditional algorithms, along with the proposed algorithms based on their pros and cons, related to Symmetric and Asymmetric Key Cryptography. 2. Comparing the importance of both of cryptographic

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

				techniques
[19]	2015 (Elsevier)	IoT	1979-2014	1. Discussing the applicability and limitations of existing IP-based Internet security protocols and other security protocols used in WSN. 2. Classifying the existing security solutions for IoT into two main types: asymmetric key schemes and pre-distribute symmetric keys to bootstrap a secure communication. 3. Comparing these schemes in terms of its efficiency, performance and security requirements.
[20]	2016 (Elsevier)	WSN	2000-2015	1. Presenting an updated survey between different Secure Group Communication (SGC) schemes in WSN. 2. Examining existing SGC schemes for both the group key management and the group member ship management, and discussing their performance and security. 3. Classifying the existing schemes of SGC into three different approaches: contributory, centralized and hybrid. 4. Providing recommendations for appropriate scheme to use for WSN . 5. Highlighting the challenges that researchers should have to address and giving them directions to potential solutions.
[21]	2016 (Elsevier)	Multi-Phase WSNs (MPW SNs).	2004-2015	1. Classifying and comparing the existing key management schemes proposed for this type of sensor network. 2. Presenting the advantages and disadvantages of each multi-phase key management scheme. 3. Giving some directions to design lightweight robust key management protocol for MPWSNs.
[22]	2017 (IEEE)	MANET	2005-2015	1. Presenting and some recent certificateless key management schemes and analyze their advantages and disadvantages. 2. Proposing a suggestion to solve the problems existing in the certificateless key management scheme.
[23]	2018 (Elsevier)	WSN	1984-2017	1. Reviewing the dynamic key management systems in WSNs and introduce some evaluation criteria in key management systems. 2. Categorizing the dynamic key management schemes based on the type of keys into key distribution mechanisms, key cryptography methods and network models.

2. KEY DISTRIBUTION TECHNIQUES

Cryptography is a field of computer science and mathematics that focuses on techniques for secure communication between two parties, and this is based on methods like encryption, decryption, signing, verification, generating of pseudo random numbers, etc [24]. Generally, there are two different schemes of cryptography: symmetric cryptography (private key cryptography) and asymmetric cryptography (public key cryptography [25].

A symmetric cryptography is also known a private key cryptography uses only a single key for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

both encryption and decryption process and only both parties who are authorized for encryption and decryption would know it [24].as we discuss briefly in section 2.1.

In asymmetric cryptography (or public key cryptography), there are two different keys used for the encryption and decryption of data as we discuss briefly in section 2.2. Also, the asymmetric cryptography has many advantages such as: providing the digital signatures and the non-repudiation, moreover increasing the level of security for large key size due to the fact that private keys do not ever need to be revealed to anyone.

Exchanging data between two parties in a secure way without any modification, or any unauthorized access needs to establish a secure connection [26] [27] [28] [29]. A secure communication must be done by exchanging a secret key between the nodes/objects in the network. Due to the fact that the majority part of IoT devices is resource-constrained devices, lightweight and scalable key distribution techniques are highly required for such devices.

The process of selecting a particular key distribution scheme to ensure security is not an easy thing because there are many factors that should be taken into account. These include the nature of the environment, the network architecture (distributed, centralized or hierarchical), and the communication mode style which may be unicast, multicast or broadcast in [17].

As we previously mentioned the IoT devices may gather, process and upload a huge amount of data to the internet. Therefore, secure communication is highly required in IoT in order to guarantee a secure exchange of data through its environment. Consequently, the process of key distribution is considered as a major part of secure communication, which provides a secure shared link between nodes in order to maintain privacy and other security issues. However the majority part of IoT devices are wireless sensors and they are considering as a limited resource devices with limited memory size, battery lifetime, communication bandwidth, and performance computing, as well as the traditional key distribution techniques are heavyweight and inappropriate for such devices, a lightweight and scalable key distribution techniques are highly required for such devices.

The strength of any cryptographic system is based on the way of how the keys are distributed and what are the encryption techniques that are used. Therefore, the process of distributing the keys can be done in different ways such as public announcement, public directories, public-key authority or public-key certificates. In the IoT environment (due to its limitations) the key distribution must be deployed in the initialization phase to reduce the overhead to these constraint devices [30].

The whole process of how to generate, store, distribute and backup the keys call the key management, so the key distribution is an important part of the key management. Moreover, there are many factors that affect the key management, such as, the key size, the key ordering sequence, and the number of alternate keys. The key size which is the number of digits that represent the key- affects the time need for encrypting and decrypting the message. Moreover, the key ordering sequence is used to prevent attacks either by generating sequential or random keys. Respectively, the number of alternate keys for varying topology change, node size and robustness and the number of trusted third parties (TTP) in key maintenance [31].

Establishing secure communication between the nodes in any network or to achieve the security services such as confidentiality, integrity, nonrepudiation authentication and others we need to distribute the keys. Therefore, the strength of any cryptographic system rests with the key distribution technique [25]. On the other hand, there are many ways to exchange or deliver the keys such as the physical delivering, but in the key distribution process we reduce the communication overhead and the complex process that in a physical way. Moreover, the key distribution scheme should take into account the constraint devises and the huge number of objects in IoT to be scalable and lightweight.

Key distribution schemes are surveyed in several papers either explicitly [17][32] or under specific concepts. Also, Key distribution schemes Key distribution schemes are mentioned under many subjects such as the key management schemes [15] [14] [13] [33] [11] [21] [23] [22] or under the challenges and issues for secure IoT [19] [3]. Some survey papers were only compared with the existing proposals for key distribution schemes in terms of many metrics such as efficiency, performance, characteristics and other metrics.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Respectively, the other are classified or divided the key distribution schemes from a different perspective, such as the encryption schemes used or the way of distributing the keys (centralized, contributory or decentralized).

The criteria for evaluating any key distribution schemes - which will be used later on in the comparisons between the schemes - are in terms of the performance and the efficiency. The performance is how this scheme being scalable, resilient and connective, while the efficiency cares about the complexity of communication, computing and the memory storage for the node.

1. Communication cost means the total number of transmitted bits used in distributing a key to establish secure connection.
2. Computation cost means the total time need to find a common key from a list of keys (searching algorithm) or the time need to compute a common key from random prime numbers as in RSA or diffie-hellman.
3. Memory Storage means the number of keys that should be stored in the memory node in order to establish a secure connection between other nodes in the network.

2.1 Symmetric-key Encryption based Schemes

A symmetric cryptography needs less computation complexity compared with asymmetric cryptography, this is why, it is widely used in IoT. Moreover, it is preferred to use for the constraint devices that have limited capabilities. Symmetric key cannot provide digital signatures because the verification process cannot be independent since the two parties are shared the same key. Therefore, if the shared key is compromised all other nodes that shared the same key will be compromised [15].

Other shortages and weaknesses for the symmetric cryptography are the connectivity and the scalability, which means the amount of preloaded information that, must be stored in a device that grows linearly with the number of potential nodes. In IoT environment the number of connected object is relatively huge.

Symmetric key distribution has two ways of exchanging the shared secret key; either by using symmetric or asymmetric encryption to exchange the key. There are many differences in viewpoints about the possibility of using symmetric key scheme over asymmetric scheme for key distribution in IoT. In [34] the recommendation about using public-key encryption based schemes are nontrivial the authors prefer the symmetric key over asymmetric, they propose a new key pre-distribution scheme was proposed to improve the network resiliency.

Basically, most of the symmetric key distribution scheme has mainly three phases: i) key predistribution, (ii) discovery the shared key and (iii) establish the path-key. During the first phase, secret keys are generated and placed on each node in advance, and then each node discovers its neighbors that are in its communication range or by any discovery algorithm. Finally, a secured link is established once they find a common secret key and the communication is done.

Previous studies proposed different classifications for symmetric key distribution schemes. In [35] the authors classified the key distribution based on the current proposals into, trusted-server schemes and self-enforcing schemes. While in [36], the key distribution schemes were classified into four kinds: probabilistic schemes, deterministic schemes, hybrid schemes and location aware or group-based schemes.

In this survey paper we differ from the other studies by classifying the symmetric key distribution schemes in IoT into three categories which are; probabilistic scheme, deterministic, and other schemes. As we discuss each of them later on in 2.1.1, 2.1.2 and 2.1.3.

2.1.1 Probabilistic Scheme

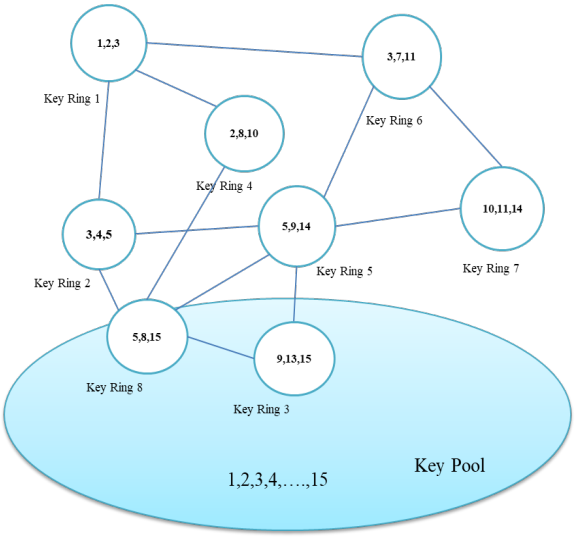
Eschenauer et al. in [37] proposed a random key predistribution scheme as shown in Figure 2 which is also called the basic scheme, this scheme based on key pool and key ring for each node and three different phases for basic scheme as shown in Figure 3. At the first phase is the initialization phase and before the sensor nodes are deployed, each node has m keys that are randomly selected from the key pool S and stored into the node's memory. The m keys are called the node's key-ring as any two key-rings will share at least with one key with probability p. In the second phase at the second phase is the key setup phase, where the node searches for its neighbors that share a key by sending broadcast message that contains short IDs assigned to each key prior to deployment. Finally, in the final phase, which is the path key establishment phase, where any two nodes that

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

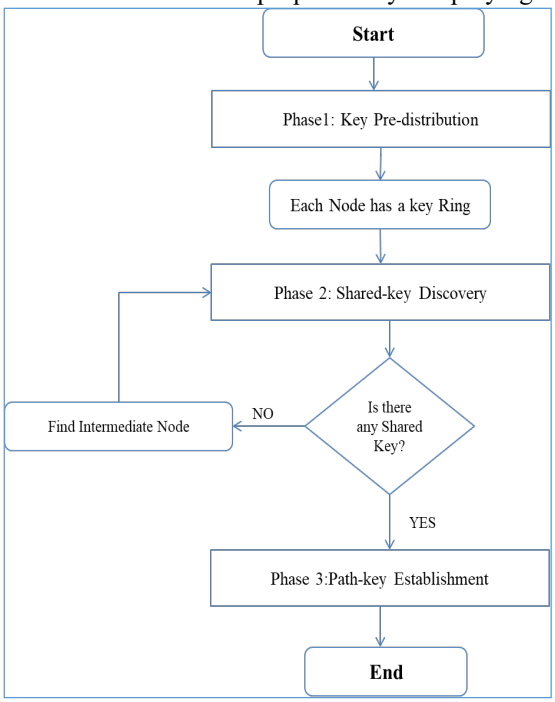
have a shared key between them will connect; otherwise these nodes can communicate securely through intermediate nodes.

Figure 2: An example of Basic Scheme

Figure 3: Random key pre-distribution Scheme



To avoid the additional time to search for common keys between the nodes, a modification of basic scheme was proposed by employing the



Merkle Puzzle in [38], namely the q-composite random key pre-distribution scheme. The modified version increases the amount of key overlap required between the nodes in the key setup phase. Instead of one key, a pair of nodes must share q keys to establish a secure link. Another improvement also for the basic scheme which is called multipath key reinforcement, basically was explored by Anderson and Perrig [39], to yield greatly improved resilience by adding some network communication overhead. Multipath key reinforcement is a method to strengthen the security of an established link key through multiple paths. Also, this method can be applied in conjunction with the basic random key scheme to yield greatly improved resilience against node capture attacks. Table 2 shows the differences between two types of probabilistic schemes based on the communication cost, computation cost and the memory storage for the node to store the keys to communicate with other nodes securely.

The probabilistic schemes depend on two factors: key pool and key ring (key chain) which is subset from the key pool assigned for each node. The challenge for the probabilistic scheme comes from how long the key ring should be and what size of key pool is used in order to provide a shared key between objects. Therefore, any two nodes that have a common key can establish a path between them. On the other hand, if there is no common key between two nodes for example, then intermediate nodes should find a common key in order to establish a secure link between these nodes. Therefore, a key path length is another problem should come up with, because of its memory storage limitations for the constraint devices. That is why, increasing the probability between the nodes to find enough numbers of shared keys for the other nodes in the network means increase the size of key ring for each is not suitable for these constraint devices and the vice versa also cause increasing the key path length which is another problem[36].

Probabilistic scheme passes through different stages of development. In each stage a new improvement has been done to deal with certain shortages or to make it compatible for certain architecture. There are many disadvantages or shortages of the probabilistic approach such as the resilience and the scalability.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table2: Different Probabilistic Key Distribution Schemes

Probabilistic Schemes / Criteria	Random key pre distribution (Basic Scheme) [15][37]	q-composite key pre-distribution [32][40]
Storage cost in each node	O(m) m: Key ring size	O(m) m: Key ring size
Communication Cost	Broadcast set of its identifiers O(m)	O(m)
Computation Cost	(Find only one shared key) Based on the search algorithm	(Find a Q- number of shared keys) Based on the search algorithm
Advantage	1. Efficient memory cost. 2. No need for intensive computation	1. Better resilience than basic scheme. In order to compromise a link key, all keys that have been hashed together must be compromised.
Disadvantage	1. IoT environment contains a huge number of objects. Therefore, this scheme is not scalable when the network size becomes huge. 2. No authentication is provided	1. The probability of being able to establish a shared key directly is smaller (it is less likely to have q common keys, than to have one). 2. Trading off between the key ring size should be increased (but: memory constraints) or key pool size should be decreased (but: effect of captured nodes)

If we talk about IoT, there are a huge number of connected objects which makes it hard to find a shared key between any two nodes. Also reducing the key path length is not an easy option in the probabilistic approach. Therefore, we should think about the ratio between the computation overhead and the communication overhead instead.

The balancing between the security level and the limited memory capacities for these constraint devices is a challenge. Meanwhile, in order to increase the security level the probability of discover the common key between the nodes should be increased through increase the key pool size , thus mean the memory storage for the node should be increased and the vice versa.

2.1.2 Deterministic Scheme

In deterministic scheme the key pool and the key ring are designed using various deterministic approaches. In contrast with or to probabilistic key distribution, in deterministic key distribution schemes the key graph is constructed in advance. Therefore, according to the edges in the key graph each node assigns the pairwise keys. Also, the aim of the proposed scheme is reducing the communication overhead because it averagely provides a shorter key path by using smaller key rings [41].

The Combinatorial design theory which is used in deterministic approach provides a method to rearrange the elements of a finite set into subsets to achieve certain properties. A Balanced Incomplete Block Design (BIBD) is the most studied type of design, which is defined as v, k and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

λ that are positive integers such that v > k ≥ 2 and A (v, k, λ) or equivalently, A (v, w, r, k, λ) Where: λ (v - 1) = r (k - 1) and w k=v r. Also, BIBD is a design (X, A) such that the following properties are satisfied where |X|= v, each block contains exactly k points, and every pair of distinct points is contained in exactly λ blocks [42]. In the symmetric BIBD (SPIBD): (w=v and thus k=r). SPIBD has four interesting properties: every block contains a group of elements; every element exist in blocks, every pair of elements exist in λ [43] [44].

Example 1: Assuming that a BIBD A (v, k, λ) = A (7, 3, 1) then X and A will be: X = {1, 2, 3, 4, 5, 6, 7} and A = {123}, {145}, {167}, {246}, {257}, {347}, {356}. Assuming that the number of nodes in the network equal 7, then each node has a key ring contains three different keys. Therefore, each node should find at least λ shared a key with other key rings. As shown in Figure 4 each node has a different key ring and shared with other nodes at least with one key.

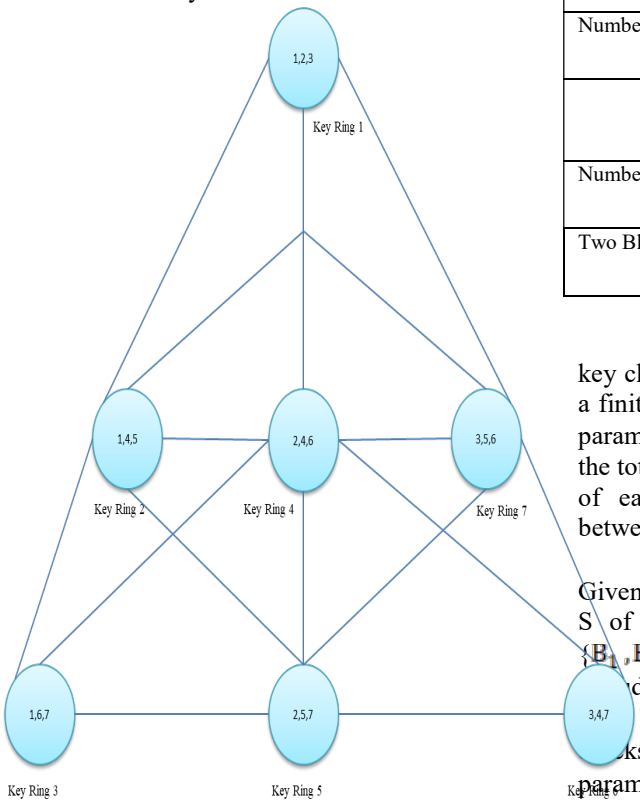


Figure 4: The Fano Plane: A (7, 3, 1)-BIBD

The mapping from symmetric design to key distribution shown in Table 3. The authors use the finite projective plane (FPP) which consider as a subset of SPIBDs and used for special interest for key pre-distribution. FPP consists of a finite set P of points and a set of subsets of P called lines. For an integer q, where q is prime and q ≥ 2, finite projective plane of order q has four properties:

(i) Every line contains exactly (q + 1) points.
(ii) Every point exists exactly (q + 1) lines.
(iii) The number of points equal (q2 + q + 1).
(iv) The number of lines equal (q2 + q + 1).

Table 3: Mapping from Symmetric Design to Key Distribution [45]

Symmetric Design	→	**Key Distribution**
Object Set (S)	→	Key-Pool (P)
Object Set Size (|S| = n^2+n+1)	→	Key-Pool Size (|P|)
Blocks	→	Key-Chains
Number of Blocks(b = n^2+n+1)	→	Number of Key-Chains (N)
Number of Blocks (b = n^2+n+1)	→	Number of Sensor Nodes (N)
Number of Objects in a Block (k= n+1)	→	Number of Keys in a Key-Chain (K)
Number of Blocks that an Object is in (r =n+1)	→	Number of Key-Chains that a Key is in
Two Blocks share (λ=1) objects	→	Two Key-Chains share (χ) Keys

If the number of lines are considered as key chains and the number of points as nodes, then a finite projective plane of order q is a design with parameters (q^2+q+1), q + 1, 1) where (q^2+q+1) is the total number of keys, (q+1) is the key-chain size of each node, and there is one common key between any two nodes [42].

Given a block design where D = (v, k,λ) with a set S of objects and of |S| =v objects and B = $\{B_1, B_2, \ldots, B_n\}$ of |B|= b blocks where each block ...des exactly k objects. Complementary Design ... has the complement blocks $\overline{B}_i = S - B$ as its ...ks for 1 ≤ i ≤ b. $\overline{D}$ S is a block design with parameters (v, b, b-r, v-k, b-2r+λ) where (b- 2r + λ > 0). If D = (v, k,λ) is a symmetric Design, then $\overline{D}$ = (v, v-k, v-2r+λ) is also a Symmetric Design.

Example 2: consider symmetric design D = (v, k, λ) = (5, 3, 2) the block of combinatory design is {1,2,3} {3,4,5} {1,3,5} {1,2,4} {2,3,4} based on the above definition v=5 objects and there

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

are b=5 blocks such that each block contains 3 objects (v- k). Also every pair of blocks intersect in b- 2r + λ = 2 objects.

In [46] two key pre-distribution schemes (KPSs) were proposed for distributed sensor networks which are: the ID based one-way function scheme (IOS) and deterministic multiple space Blom's scheme (DMBS).The aim of the proposed approaches are enhancing the resilience against coalition attack and obtaining perfect scalability than other randomized approaches.

In [47] a combinatorial design theory was applied to pre distributed Blundo's polynomials in mobile sensor network, to increase the scalability of polynomial. As shown in Table 4 a comparison was made between different deterministic proposals [36][48][49][50][47].

Different metrics were used such as the memory storage, communication cost and the computation cost for the proposed schemes. Also, the several proposals aim to increase the scalability of the network and to increase the resilience against the attack. The deterministic scheme comes to improve the scalability of the network and to reduce the memory storage. But, many deterministic approaches are based on the combinatorial design theory which has the main drawbacks that come from the difficulty of their construction.

2.1.3 Other Schemes

The other schemes are sometimes the mixture between different probabilistic schemes, or the combination between the probabilistic approach and the deterministic approach to take the advantages from both of them. Such benefits are to make the balancing between the levels of security and enhancing the scalability, resilience and the memory storage for the nodes in the network. In Table.4 other symmetric key distribution schemes are compared with each other in terms of the communication cost, computation cost, memory storage, cons and pros for each of them.

In [52] a hybrid scheme was proposed based on combinatorial design keys and pair-wise keys. There scheme aimed to ensure high resiliency against sensor nodes compromised in the network and to reduce the memory storage in each node. Also, the proposed approach divides the WSN into cells, and using a combinatorial design for intra-cell communication into each cell due to key storage overhead, while using pairwise keys for inter- cell communication.

In [53] a computationally efficient construction for the symmetric matrix-based key distribution was introduced.
The proposed scheme aimed to reduce the computation complexity overhead for generating the key information and to reduce the memory overhead in small network. Other schemes such as Logical tree based key pre-distribution schemes and entity based t are based on trusted party. Moreover, it has shortages which are not scalable and not resilience.

Table 4: Different Deterministic Key Distribution Schemes

Deterministic Schemes / Criteria	[47]	[48]	[49]	[50]	[51]	[36]
Storage cost in each node	n+1 t-polynomial-set O(k)	$O(\sqrt[k]{N})$ Where k: A t-degree (k+1)-variety symmetric polynomial is used	s + 1 The size of key chain for the each node	$\frac{r}{2}+1$	$(t+1)\log q$ t: degree of polynomial q: prime number	3n keys and n^2 location information
Communication Cost	$(n+1)$	$\frac{K(N_1^{k-1}-1)(N_1-1)}{N_1^{k}-1}$ Where N= N_1^{k}	Low	Low	Low communication overhead	No communication overhead
Computation Cost	Low	$2^{\sqrt[k+1]{\frac{k(k+1)!}{2}}\sqrt[k]{N}+}$	Low	Low	Large t means high computation cost, while small t means low	n^2-1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

					computation cost.	
Advantage	Improve network scalability Enable authentication Moderate resiliency in the presence of wise attackers.	1. Scalable for large scale networks. Very small memory cost per node.	1. Minimize the keychain size. 2 .Maximizing pairwise key sharing probability and resilience. 3.Minimizing average key-path length.	Reduce the number of keys per node. Perfect resilience.	Unconditionally secure for up to t compromised nodes.	Better resilience and the distribution technique ensures 100% connectivity.
Disadvantage	local secure connectivity	local secure connectivity	local secure connectivity	Not suitable for large size network.	1.It can only tolerate no more than t compromised nodes. 2.t is limited by the memory available in sensor nodes	Not suitable for large size network.

Table 5: Different Other Key Distribution Schemes

Other Schemes / Criteria	[53]	[54]	Entity based or arbitrated schemes	[52]
Storage cost in each node	i^{th} row of secret matrix and i^{th} column of public matrix $(t+1)$	$\log_2 n$	In GC node O(n) Other nodes	Very low The node stores only the shared keys with the cell members.
Communication Cost	Low	O ($2 \log_2 n$)/ For rekeying	O(n) for the group entity	inter-cell+ intra cell communication overhead
Computation Cost	compute a shared key K_{ij} i computes $A(i,.)G(.,j) = K_{ij}$	Low	No computation overhead in other node	The time for compute the shared key with other nodes
Advantage	Efficient memory storage in the node for small λ	Efficient memory storage	1. Good scalability. Each node needs little memory.	1. low storage overhead 2. high resiliency
Disadvantage	1. Has the λ security. In other words, if more than λ rows are	Costly rekeying	1. All key are exposes if the master key	1. The construction for the

	compromised, the entire secret matrix can be compromised Also, not scalable for large size of network.		compromises. 2. Bottleneck onto central node. 3. Not efficient in the large network. More expensive re-keying	combinatorial design. 2. Design for certain area and divided it into equal-size cells. which is not IoT

2.2 Asymmetric-key encryption based Schemes

Public key cryptography is widely used in the realm of the internet. Also, this scheme provides strong security and enough scalability, but the public key cryptography needs high cost computational complexity. On the other hand, some researchers believe that public key cryptography is too heavy-weight for constraint devices such as sensor nodes because of its high computation complexity. Therefore, modifying the traditional public key cryptography for these constraint devices is the solution. A lightweight ECC and RSA can offer equivalent security with substantially smaller keys, for example, a in ECC 160-bit key are expected to offer comparable security with an RSA 1024-bit key [55][56] .

Other researchers believe that the technology is expected to be developed and the next generation of these constraint devices will cover the limitations for current devices. Therefore, with the fastest growing technology, the public key schemes are no longer impractical and will be widely used in these constraint devices as the near future.

Many previous studies show the applicability of using public key cryptography over the constraint devices [57] [58] [59][60]. In [57], the authors show that public key schemes are applicable on a sensor node. They show in spite of the computational cost, it is expected to fall faster than the communication and storage cost. In [58] the authors show the applicability of applying public keys on small devices without hardware acceleration and show the relative performance advantage of ECC over RSA. In [60] a comparison was made between RSA and ECC techniques. The analytical results showed that ECC takes less time for encryption and decryption and also provides keys of smaller sizes as compared to RSA.

Other opinions are about the preference of using public key cryptography over the symmetric key cryptography in the constraint devices network such as WSN. The symmetric encryption technique required less computation time while this will lead to introduce a complicated key management system and also need a larger memory to store all other keys for all other nodes in the network. In [61] lightweight elliptic curve cryptography (ECC) is implemented on WSN. Also, it was compared with the symmetric-key. The results show the efficiency of ECC over symmetric key.

The common perception about the public key cryptography is the computationally complexity which is expensive compared with the symmetric approaches. In asymmetric key technology the management is easier and more resilient to node compromise than symmetric key technology. Recently, some researchers began to investigate the feasibility of using asymmetric key technology on the constraint devices because of the rapid advances in its hardware capability [14]. Table.6 present different asymmetric key algorithm in terms of the features, the security solution that provides and its cons and pros.

Secure group communication is used in many important applications. Therefore, there are many applications in IoT that are based on this type of communication. A group key agreement (GKA) is a secure and robust approach to establish a secure connection through the network channel. In [63] a lightweight asymmetric group key agreement was proposed to reduce the computation overhead to overcome the resource constraint of mobile terminals. The authors have the main contribution by proposing an authentication protocol which was

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

called ABE-AAGKA. Therefore, the authentication protocols need key establishment.

Designing a lightweight public key cryptography for IoT environment is must due to the limited capabilities for the constraint devices. Thus, the cost of computation complexity, communication cost, or storage requirement will be reduced. Also, using a PKC enhances the scalability of the network i.e. to support a huge number of objects that connect in the networks or to deal with the dynamic changing in the network topology. Another object is to enhance the resilience against the node attacks or the key compromise.

In [64], a lightweight key establishment protocol based on ECC was proposed, which combined ECDH with symmetric cryptography and hash chain. Their approach is based on initialization phase and key establishment phase. In the initialization phase and before the deployment of sensors, a preload same initial key Kn for every node as initial trust. After that, two nodes will use their initial key to perform pairwise key establishment.

Table 7 compares between different asymmetric key distribution based on different network types such as WSN, traditional network or IoT. Also, the comparison is done based on the way the keys are distributed such as centralized, decentralized or distributed. In [65] [66] the computation over head is reduced to be moderate, while in [33] the computation overhead is relatively high because of the powerful devices powerful devices in the traditional network. Furthermore, all these proposals ensure the flexibility, scalability and robustness for the network.

Table 6: Comparison between Different Asymmetric Key Algorithms

Asymmetric Key Algorithm	Features	Security Solutions	Advantages	Disadvantages
RSA	It consists of two parameters one used for the private key and the other represents the public key. [18].	To provide enough level of security the key size should be larger than 1024 bits [18].	Providing the nonrepudiation property and It is difficult to produce the private Key from the public key.	Very slow key generation and slow signing and decryption.
ECC	It computes the keys through elliptic curve equations [18].	Introduction of Elliptic Curve Digital Signature Algorithm (ECDSA) [18] it protects against Man in-the-Middle attacks.	Giving the same level of security as RSA with small key size which is 164 bit [18].	More complex to implement than other schemes and increase the complicity of the encrypted message.
Diffie-Hellman	It is based on sharing the secret cryptographic key. This key is used for both encryption and decryption purposes. It relies on hardness of the discrete logarithms [18].	Needing permanent key update for to defeat the Man in the Middle attacks.	Providing enough level of security with a small size of key 256 bit.	Cannot be used for signing digital signatures.
Digital Signature (DSA)	It consists of a pair of large numbers, computed based on some algorithms to authenticate data [56]. The signatures are generated through private keys and are verified using public keys. [62].	Verification software is necessary. Also, digital certificates should be bought from trusted authorities..	Providing authentication, nonrepudiation. Also, don't need huge computation complicity.	A short life span and complicate sharing.

Table 7: Different Asymmetric Key Distribution Scheme

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Ref (Year)	Network Type	Asymmetric Key Distribution Scheme	Group key Distribution approaches	Communication Cost	Computation Cost
[56] (2009)	Distributed Sensor Network(DSN)	ECC	Centralized	Equivalent with the cost of the [61] protocol.	Enhancing 17% over [61]
[68] (2014)	not specific	ECC	Distributed	Low	(n − 1)E. + (n + 1)SM.
[69] (2015)	Smart Grid	asymmetric key-wrapping	Centralized	(Y, C, T) the bit length of Y depends on the group G, while the size of C depends on the size of the input data key. the length of authentication tag T	At Server side generating two hash values and two exponentiations + Performing ENC and MAC once respectively.
[65] (2015)	Dynamic wireless sensor networks	Public key & pairwise key	Decentralized	Low	Moderate
[66] (2017)	IoT	Public key (RSA)	Centralized	Low	taking only 82% of Std. RSA and 24% of ESRKGS times
[33] (2018)	Traditional Network	Public key (RSA)	Centralized	Low	High

2.3 Hybrid Key Distribution Encryption Based Schemes

The hybrid scheme is to make a mixture of symmetric and asymmetric key distribution schemes. In IoT a hybrid scheme aims to distribute the cost of computation, communication and the memory storage overhead onto the difference capable devices and to take the benefits from both of them. Therefore, the previous proposals studied the different capabilities in IoT environment, and they preferred to apply the traditional schemes from symmetric and PKC -which need high computational complexity- on the powerful devices. On the other hand the light weight key distribution schemes were designed and applied on constraint devices.

In [67] hybrid authenticated key establishment protocol for self-organizing sensor networks was proposed.
It combined the symmetric key and ECC. The high cost for public key operation was replaced with the symmetric key in the sensor node side by using ECC to perform security functions on sensors with limited computing resources. Also, there are many studies that proposed a hybrid scheme in WSN, in [70], a hybrid design of key pre-distribution which is a combinatorial design followed by a heuristic is applied.

The quantum key distribution mechanisms are highly secured and they prevent several attacks by exchanging secret keys in the quantum channel. Also, hybrid approaches were proposed in [71][72] by combining both quantum cryptography and classical cryptography, to provide secure communications and prevent replay attacks, man-in-the-middle attacks, and passive attacks over networks. Also the hybrid approaches were designed for wireless LAN and traditional networks so they are not design for constrained devices.

Table 8 summarizes some of the previous studies that proposed hybrid approaches and compares them in terms of the environment applied on, the approaches from which the techniques are combined, and the security requirements were achieved by the proposals such as integrity, authentication and confidentiality. Each proposed scheme has its own cons and pros for example, in [74] the authors proposed a hybrid approach mixed between symmetric key and public key for WSN. In this approach each sensor should keep all other public keys used which will lead to increasing the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

memory storage at each node. Therefore, their scheme is not scalable when the network size becomes large. While in [71] the hybrid technique is proposed for traditional network which is considered as powerful capable devices on the contrary of WSN that needs less computational cost and is limited in memory storage. Other studies [75][74] try to keep the balance between the memory storage at each node and the resilience against node or key attack. While the other try to achieve certain security requirement such as the authentication, digital signature and other.

Table 8: Different hybrid schemes for Key Distribution

Ref	Year	Environment	Hybrid Scheme	Reducing Memory overhead	Resiliency	Scalability	Security Requirement
[56]	2009	DSN	ECC+ Symmetric Key	√	√		Authentication
[73]	2010	*Ad hoc networks.*	Public Key+ Symmetric key				Authentication
[74]	2014	*WSN*	Public Key + Session Key (Energy)	√ Only 4 Keys stores	√	√	Authentication
[71]	2015	Traditional Network	Quantum and classical data.		√		All
[72]	2015	WLAN	Combinatorial design +heuristic approach		√		√
[75]	2015	WSN	Q-Composite Key distribution scheme + Polynomial Pool-Based Scheme	√	√		Authentication
[35]	2016	WSN	Public Key + Symmetric Key	√			confidentiality and authentication.
[76]	2017	Hierarchy WSN	Symmetric and asymmetric key distribution based on the additional commodity hardware trusted platform model.		√	√	confidentiality ,integrate and authentication.

Table 9 classifies the symmetric, asymmetric and the hybrid key distribution in terms of the architecture, the security level, the security requirements, scalability and the computation complexity for each one. The architectural is referring to how the key distribution process is performed, and consequently, these techniques are classified into hierarchical, decentralized, centralized and distributed. Also, the nature of the network which could be homogeneous such as WSN or heterogeneous such as IoT environment. Also, all security attacks aim to compromise the key for the nodes regardless of what is the key distribution encryption techniques that are used.

In the summary we should take the limitation of IoT environment like the different capabilities and different technologies. Therefore, the designed approach should achieve the resiliency against the node or the key attack, and the scalability because the nature of IoT which linked huge number of objects together. Also, it should be reducing the memory storage and computation and communication overhead due the limited capabilities for the constraint devices.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 9: Classification of key distribution according different parameters

Key Distribution Scheme			
	Symmetric	**Asymmetric**	**Hybrid**
Architecture	Centralized / Decentralized Distributed	Centralized / Decentralized	Hierarchical / Decentralized/ Centralized
Security Level	High	Moderate	Moderate to high
Security Requirement	Confidentiality, Authentication	Digital Signature , Confidentiality and Authentication.	Digital Signature , Confidentiality and integrate Authentication
Scalability	No	Yes	Yes
Computation Complexity	Low	High	Moderate
Nature of the Network	Homogeneous	Homogeneous	Homogeneous/ heterogeneous
Security Attacks	Man in the middle attack; Node Compromising; Eavesdropping; Malicious nodes; Impersonation		

3. COMPARISIONS AND RECOMMENDATIONS

Based on the previous studies that have been done, we found that the symmetric key distribution schemes are dependent on many parameters. These parameters should be taken into consideration to select the suitable symmetric key distribution approach in IoT. The first parameter is the size of the network which is in terms of the number of connected devices (large or small). Also, the network topology nature that could be either stationary or very dynamic i.e. if the connected devices are in fixed locations we consider the network as stationary while if these objects change frequently their position or it is a mobile object, here we consider the network type as very dynamic.

The communication style between these objects is another factor that should be taken into consideration like pair-wise (unicast), group-wise (multicast) or network-wise (broadcast) all these parameters are determined which keying style should be taken. We propose a new taxonomy in Figure 5 for the appropriate symmetric key distribution schemes which are probabilistic, deterministic and other schemes based on the network size, network type and the communication style. We found in the small network and also stationary any symmetric schemes are fit. Also, in large networks the probabilistic scheme is not appropriate, because it needs to increase both the key pool and the key rings to provide shared keys between the objects which are inappropriate for memory storage in constraint devices.

In the dynamic network nature, the network-wise key is replaced in group-wise because there are many objects changing their positions, so there is always a new member joining and other members leaving. When the network size becomes large and the network type becomes dynamic we need to select a scheme that achieves the following points:

1. The scalability of the network, because of the large number of connected objects and continues changing for the objects too.
2. The resilience of the network against the node attacks.
3. The rekeying problem should be taken to ensure both forward and backward secrecy.

We prefer the hybrid scheme and the deterministic approaches over the probabilistic schemes, because of the memory storage limitation for these constraint devices. To increase the probability of having common keys between the members in the network both the key pool and the key ring should

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

be increased. This solution is not appropriate for the memory limitation.

The public key cryptography relatively needs high computational complexity. On the other hand it is better in terms of scalability, connectivity and better in key distribution mechanism than a symmetric key encryption. Based on the previous studies that were made on different environment always a customization of public key distribution must be done to be lightweight in order to fit into the limited capabilities of the IoT devices. Also, many proposals used the public key only at first step to establish a shared key between the nodes. A comparison was made between different studies that proposed symmetric, asymmetric or hybrid key distribution scheme as shown in Table 10 and discussed these schemes in terms of different evaluated models as following:

(a) Performance analysis by analyzing the computation and communication overhead or memory storage space. Also, the resiliency or the scalability of the proposed scheme.

(b) Implementation using a particular programming language, a prototype, or test bed.

(c) Simulation using a particular network simulator.

(d) Theoretical using a formal equation to evaluate and analysis of the proposed approach

Table 10: Comparison between different Key distribution schemes According to the Used Evaluation Model

Ref / Evaluation Model	[71] [72] [77]	[70]	[36][46][47] [48][52][75]	[35]	[49]	[56][61][74]
Performance analysis			√		√	√
Implementation		√				
Simulation		√	√	√		√
Theoretical evaluation	√		√		√	

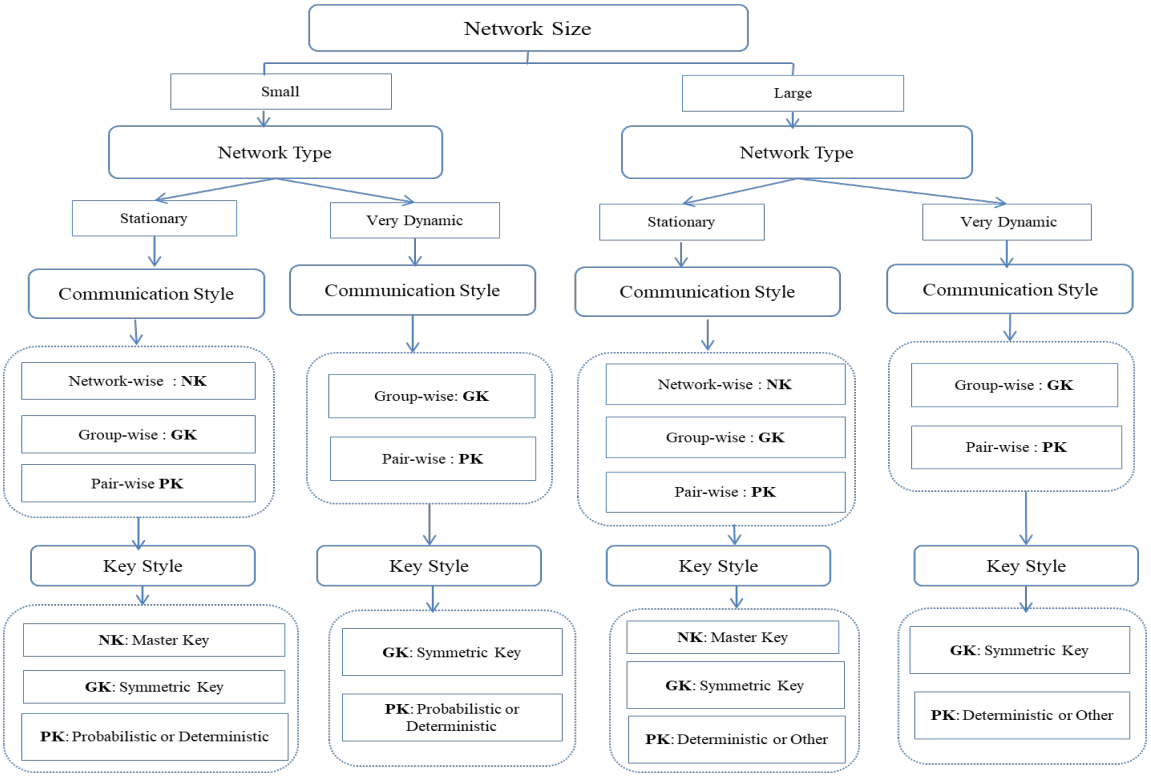


Figure 5: Taxonomy for Different Symmetric key Distribution Scheme

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. PROPOSED ARCHITECTURE

Based on the previous surveys that have done about the key distribution schemes in IoT, many challenges and issues were found. These may include the nature of the network that is heterogeneity as it contains different types of networks such as WSN, LAN, MAN, AdHoc , MANET, etc, and different types of technologies. Also, in IoT environment there are a lot of connecting objects enough and the topology of the network is not stable while it contains many changing objects (leaving and joining), so any design for key distribution scheme should take these issues into consideration.

4.1 The Difference between Current Literature

Many proposals in key distribution filed try to enhance protocols, techniques and approaches to ensure an acceptable security level in the IoT environment. Therefore, the need to provide enough level of security under many limitations for these environments, is not an easy approach. Table 11 illustrates different key distribution protocols compared with each other, in terms of the deployment mechanism for the IoT devices of the network that may be (centralized, distributed, clustering, hierarchy or regular regions). Also, the type of nodes in the network was taken from the powerful capabilities perspective. Furthermore, the phases for each protocol in key distribution and the number of stored keys at the initialization phase are shown.

Table.11 Different Key Distribution Protocols

[Ref](journal)	Deployment mechanisms	Types of nodes	Proposed Scheme phases	Number of keys before the key establishment phase
[64](IEEE)	Distributed	1 .Sensor node. (s_n)	1. Initialization phase 2. Key establishment phase 3. Node join phase	initial key k_n
[78](IEEE)	Distributed	1 .Sensor node. (s_n)	1. Predistribution Phase 2. Initialization Phase 3. Key Establishment Among Nodes Within the Initialization Phase 4. Key Establishment Between a Node Within the Initialization Phase and One in the Working Phase	• The proper ring of seeds (where each seed is matched to an ID). • The functions F()and t(). • Master key (MK) • node identifier (ID) • The parameters μ and τ
[79](Springer)	(Distributed)Based on the transmission range	1.Base station (BS) 2. Sensor node.(s_n)	1. Key Establishment. 2. Key refreshes phases. 3. Adding a new node.	First term and recursive formula.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[80] (Elsevier)	Clusters	1.Base station (BS) 2.cluster head (CH) 3. Sensor node (S_n)	Neighbor discovery Clustering Triple key generation Polynomial based triple key generation	Identity (ID)
[81](IEEE)	Distributed	1. Sink node. 2. Sensor node (S_n)	3. Predistribution Phase. 4. Key Establishment. 5. Storing Organization 6. Key Update	Ring of key and unique identifier (ID*i*).
[76] (IEEE)	Clusters	1.Base station (BS) 2.cluster head (CH) 3. Sensor node (S_n)	1. Installation. 2. Secure boot. 3. Symmetric key generation. 4. A symmetric key generation.	Not mentioned
[82](IEEE)	Clusters	1.Base station (BS) 2.cluster head (CH) 3. Sensor node (S_n)	1. Pre-distribution. 2. Cluster formation phase. 3. Steady state phase	n partial keys,
[83](WILEY)	m-ary-tree of a depth h^{26}	1. Leaf nodes 2. Interme diate nodes. 3. Root is the top level.	1. Key Establishment. 2. Key Update phases.	Secret key(SK) Multicast key(KI)
[84] (Elsevier)	Region cells	1. Head node 2. Sensor node (S_n)	1. Key pre-distribution for intra-cell communication 2. Key pre-distribution for inter-cell communication 3. Shared key discovery in the network.	Pair wise key

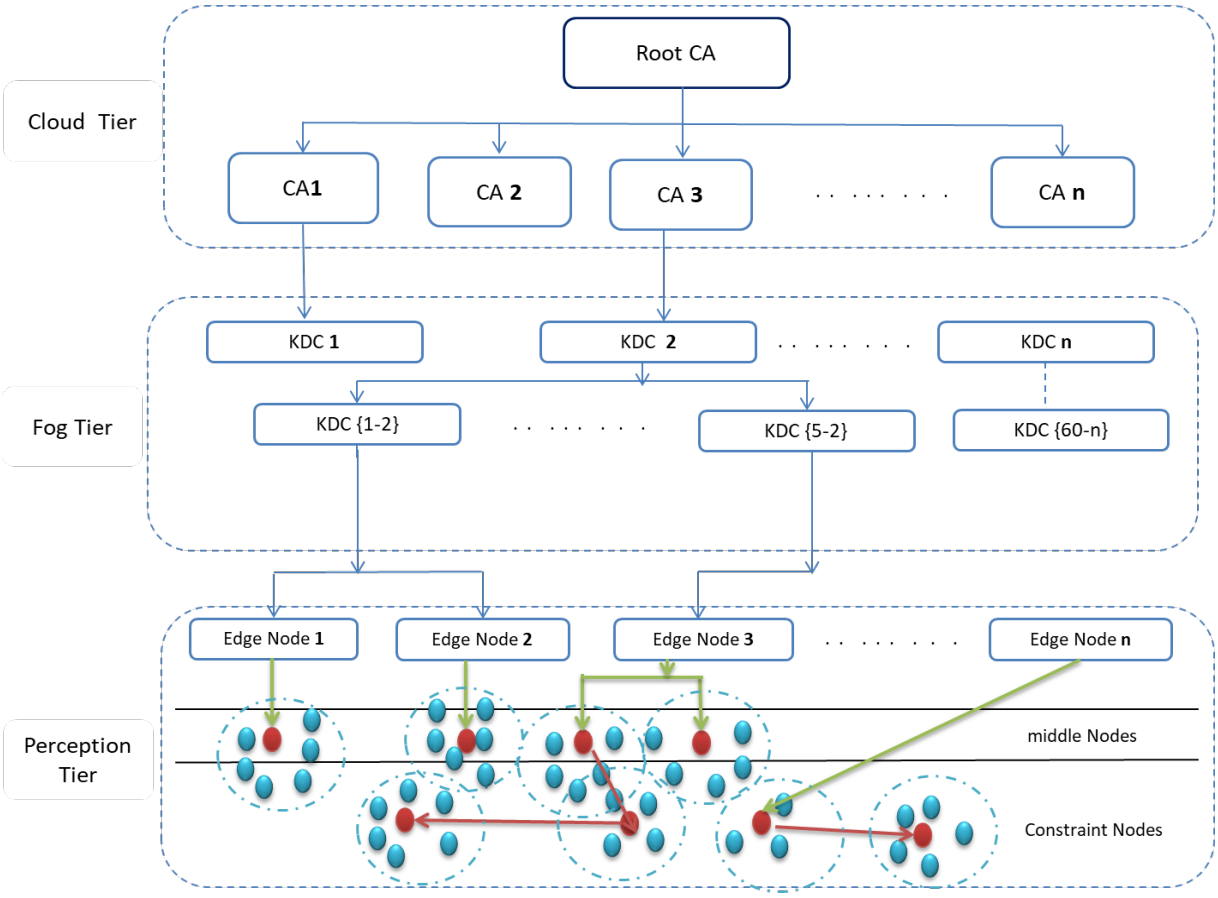
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fog cloud IoT (FCIoT) architecture is considered as one of the promising technologies that provide a scalable construction, especially in IoT applications. Fog cloud IoT was found to increase the performance and energy efficiency and to reduce the latency to get high response time. The previous studies didn't mention the key distribution in FCIoT architecture as a whole system, but they only studied the key distribution schemes on each layer individually. We present anew key distribution in Figure 6 for Fog Cloud IoT architecture as a whole; there are three layers with different capabilities, different natures, and different data types. Therefore the key distribution scheme should deal with these three layers together.

Regarding the cloud layer, a high capability layer in storage and processing- root certificate authority was suggested to be contained in this layer in hierarchical architecture in order to support the scalability. On the other hand, this certificate authority supports trusted authority and key distribution center (KDC) which are responsible to generate public and privet keys for edge nodes included in the perception layer. The perception layer is organized also as a hierarchical structure and contains three different types of nodes; constraint nodes, intermediate nodes, and edge nodes. The constraint node may be a sensor node or RFID or any limited resources node, so the key distribution scheme that is used should be lightweight to fit the characteristics of these devices. Also should have less cost in communication and computation.

Intermediate node depends on the power of that node, it may use either lightweight key distribution or traditional key distribution schemes based on its capabilities. Moreover, the shared key that is established between different fog nodes is differing in that key which is used to establish a shared key between different edges nods. Any to nodes locate with indifferent edge nodes and these edge nodes also locate in different fog nodes a hierarchy common key should be established.

Figure 6: Proposed Key Distribution for Fog cloud IoT (FCIoT) Architecture



ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. CONCLUSION

Providing security in any network should be done based on key distribution protocols that pave the way to achieve a secure link between remote nodes. Internet of Things contains powerful nodes as well as limited capabilities nodes that have low memory space, low computation power, limited power supply, and limited bandwidth. In order to serve limited capability devices in IoT, many light weight key distribution schemes have been proposed. In this paper, we analyzed and compared the existing IoT key distribution network schemes and categorized them based on the cryptographic method used. Based on the resulted observation and derived recommendation, we proposed a hybrid hierarchical key distribution architecture in the context of an IoT that adapt to the current technologies of could and fog computing specifications.

REFERENCES

[1] Luigi Atzori, Antonio Iera, and Giacomo Mora- bito. Understanding the internet of things: def- inition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, 56:122–140, 2017.

[2] Huda Saadeh, Wesam Almobaideen, Khair Eddin Sabri, and Maha Saadeh. Hybrid sdn-icn architecture design for the internet of things. In *2019 Sixth International Conference on Software Defined Systems (SDS)*, pages 96–101. IEEE, 2019.

[3] Wesam Almobaideen, Mohammad Qatawneh, and Orieb AbuAlghanam. Virtual node schedule for supporting qos in wireless sensor network. In *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, pages 281–285. IEEE, 2019.

[4] Hadeel Alazzam and Wesam Almobaideen. Enhancing the lifetime of wireless sensor network using genetic algorithm. In *2019 10th International Conference on Information and Communication Systems (ICICS)*, pages 25–29. IEEE, 2019.

[5] Shancang Li, Li Da Xu, and Shanshan Zhao.

The internet of things: a survey. *Information Systems Frontiers*, 17(2):243–259, 2015.

[6] Sanad AbuRass and Mohammad Qatawneh. Performance evaluation of aes algorithm on supercomputer iman1. *International Journal of Computer Applications*, 975:8887, 2018.

[7] Ammar Gharaibeh, Mohammad A Salahuddin, Sayed Jahed Hussini, Abdallah Khreishah, Issa Khalil, Mohsen Guizani, and Ala Al-Fuqaha. Smart cities: A survey on data management, security, and enabling technologies. *IEEE Communications Surveys & Tutorials*, 19(4):2456–2501, 2017.

[8] Maha Saadeh, Azzam Sleit, Khair Eddin Sabri, and Wesam Almobaideen. Lightweight identity based signature for mobile object authentication in the internet of things. *Journal of Theoretical Applied Information Technology*, 96(3), 2018.

[9] Wesam Almobaideen and Maha Saadeh. Lightweight authentication for mobile users in the context of fog computing. *International Journal of Advanced Computational Engineering and Networking*, 6(12):2321–2063, 2018.

[10] Huda Saadeh, Wesam Almobaideen, and Khair Eddin Sabri. Ppustman: Privacy-aware publish/subscribe iot mvc architecture using in- formation centric networking. *Modern Applied Science*, 12(5):128, 2018.

[11] Pratik P Chaphekar. Survey of key distribution schemes for wireless sensor networks. *arXiv preprint arXiv:1405.4286*, 2014.

[12] Sandro Rafaeli and David Hutchison. A survey of key management for secure group communication. *ACM Computing Surveys (CSUR)*, 35(3): 309–329, 2003.

[13] Hung Le Xuan, Sungyoung Lee, and Young-Koo Lee. A key-exchanging scheme for distributed sensor networks. In *Intelligence in Communica- tion Systems*, pages 271–279. Springer, 2005.

[14] Anne Marie Hegland, Eli Winjum, Stig F Mjolsnes, Chunming Rong, Oivind Kure, and Pal Spilling. A survey of key management in ad hoc networks. *IEEE Communications Surveys & Tutorials*, 8(3):48–66, 2006.

[15] Yun Zhou, Yuguang Fang, and Yanchao Zhang. Securing wireless sensor networks: a survey. *IEEE Communications Surveys & Tutorials*, 10 (3), 2008.

[16] Junqi Zhang and Vijay Varadharajan. Wireless sensor network key management survey and taxonomy. *Journal of network and computer applications*, 33(2):63–75, 2010.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[17] Chi-Yuan Chen and Han-Chieh Chao. A survey of key distribution in wireless sensor networks, security and communication networks, 2011.

[19] survey of symmetric and asymmetric key cryptography. In *Electronics, Communication and Computa- tional Engineering (ICECCE), 2014 Interna- tional Conference on*, pages 83–93. IEEE, 2014.

[20] Kim Thuat Nguyen, Maryline Laurent, and Nouha Oualha. Survey on secure communication protocols for the internet of things. *Ad Hoc Networks*, 32:17–31, 2015.

[21] Omar Cheikhrouhou. Secure group communica- tion in wireless sensor networks: a survey. *Jour- nal of Network and Computer Applications*, 61: 115–132, 2016.

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

[23] Qi Liu and Xiangyu Bai. Survey on certifi- cateless key management schemes in mobile ad hoc networks. In *Electronics Information and Emergency Communication (ICEIEC), 2017 7th IEEE International Conference on*, pages 334–

339. IEEE, 2017.

[24] Mohammad Sadegh Yousefpoor and Hamid Barati. Dynamic key management algorithms in wireless sensor networks: A survey. *Computer Communications*, 2018.

[25] William Stallings, Lawrie Brown, Michael D Bauer, and Arup Kumar Bhattacharjee. *Computer security: principles and practice*. Pearson Education, 2012.

[26] William Stallings. *Cryptography and network se- curity: principles and practice*. Pearson Upper Saddle River, NJ, 2017.

[27] Mohammad Qatawneh Heba Harahsheh. Performance evaluation of blowfish algorithm on supercomputer iman1. *International Journal of Computer Applications*, 10(2), 2018.

[28] Areej Al-Shorman and Mohammad Qatawneh. Performance of parallel rsa on iman1 supercomputer. *International Journal of Computer Applications*, 180(37):31–36, Apr 2018. ISSN 0975-

8887. doi: 10.5120/ijca2018916733.

[29] Mais Haj Qasem and Mohammad Qatawneh.

[18] Sourabh Chandra, Smita Paira, Sk Safikul Alam, and Goutam Sanyal. A comparative

Parallel hill cipher encryption algorithm. *International Journal of Computer Applications*, 179 (19):16–24, 2018.

[30] Amaal Shorman and Mohammad Qatawneh. Performance improvement of double data encryption standard algorithm using parallel computation. *International Journal of Computer Applications*, 179(25):1–6, Mar 2018. ISSN 0975- 8887. doi: 10.5120/ijca2018916527.

[30] Monjul Saikia and Md A Hussain. Improving the performance of key pre-distribution scheme in sensor network using clustering of combinatorics. In *Computing, Communication and Au- tomation (ICCCA), 2016 International Confer- ence on*, pages 682–686. IEEE, 2016.

[31] M Bala Krishna and M Doja. Symmetric key management and distribution techniques in wire- less ad hoc networks. In *Computational intel- ligence and communication networks (CICN), 2011 international conference on*, pages 727–731. IEEE, 2011.

[32] Haowen Chan, Adrian Perrig, and Dawn Song. Key distribution techniques for sensor networks. In *Wireless sensor networks*, pages 277–303. Springer, 2004.

[33] Vinod Kumar, Rajendra Kumar, and SK Pandey. A computationally efficient centralized group key distribution protocol for secure multicast communications based upon rsa public key cryptosystem. *Journal of King Saud University-Computer and Information Sciences*, 2018.

[34] Wenliang Du, Jing Deng, Yunghsiang S Han, Pramod K Varshney, Jonathan Katz, and Aram Khalili. A pairwise key predistribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, 8(2):228–258, 2005.

[35] Ramu Kuchipudi, Ahmed Abdul Moiz Qyser, and VVSS S Balaram. An efficient hybrid dynamic key distribution in wireless sensor networks with reduced memory overhead. In *Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on*, pages 3027–3030. IEEE, 2016.

[36] Md Abdul Hamid, Mohammad Abdullah-Al-Wadud, Mohammad Mehedi Hassan, Ahmad Al-

mogren, Atif Alamri, Abu Raihan M Kamal, and Md Mamun-Or-Rashid. A key distribu- tion scheme for secure communication in acous- tic sensor networks. *Future Generation Com- puter Systems*, 86:1209–1217, 2018.

[37] Laurent Eschenauer and Virgil D Gligor. A key- management scheme for distributed sensor net- works. In *Proceedings of the 9th ACM Confer- ence on Computer and Communications Secu- rity*, pages 41–47. ACM, 2002.

[38] Ralph C Merkle. Secure communications over insecure channels. *Communications of the ACM*, 21(4):294–299, 1978.

[39] Ross Anderson, Haowen Chan, and Adrian Per- rig. Key infection: Smart trust for smart dust. In *Network Protocols, 2004. ICNP 2004. Proceed- ings of the 12th IEEE International Conference on*, pages 206–215. IEEE, 2004.

[40] JianBo Fu, QiaoLian Li, Sujun Li, and Lawrence Ssanyu. A modified q-composite random key predistribution scheme based on kryptograph. In *Computer Application and System Modeling (ICCASM), 2010 International Conference on*, volume 15, pages V15–240. IEEE, 2010.

[41] Seyit A Camtepe and Bülent Yener. Combina- torial design of key distribution mechanisms for wireless sensor networks. In *European Sympo- sium on Research in Computer Security*, pages 293–308. Springer, 2004.

[42] Douglas R Stinson. Introduction to balanced in- complete block designs. *Combinatorial Designs: Constructions and Analysis*, pages 1–21, 2004.

[43]R Julian R Abel, Andres E Brouwer, Charles J Colbourn, and Jeffrey H Dinitz. Mutually or- thogonal latin squares (mols). *The CRC Hand- book of Combinatorial Designs,*, 1996.

[44] Walter Denis Wallis. *Combinatorial designs*.

CRC Press, 1988.

[45] Seyit A Çamtepe and Blent Yener. Combina- torial design of key distribution mechanisms for wireless sensor networks. *IEEE/ACM Transac- tions on networking*, 15(2):346–358, 2007.

[46] Jooyoung Lee and Douglas R Stinson. Determin- istic key predistribution schemes for distributed sensor networks. In *International Workshop on Selected Areas in Cryptography*, pages 294–307. Springer, 2004.

[47] David Sanchez Sanchez and Heribert Baldus. A deterministic pairwise key pre-distribution scheme for mobile sensor networks.In *Secu- rity and Privacy for Emerging Areas in Commu- nications Networks, 2005. SecureComm 2005. First International Conference on*, pages 277–

288. IEEE, 2005.

[48] Yun Zhou and Yuguang Fang. Scalable and de- terministic key agreement for large scale net- works. *IEEE Transactions on Wireless Commu- nications*, 6(12), 2007.

[49] Seyit Ahmet Camtepe, Bulent Yener, and Moti Yung. Expander graph based key distribution mechanisms in wireless sensor networks. In *Communications, 2006. ICC'06. IEEE Interna- tional Conference on*, volume 5, pages 2262–2267. IEEE, 2006.

[50] Zhen Yu and Yong Guan. A robust group- based key management scheme for wireless sen- sor networks. In *Wireless Communications and Networking Conference, 2005 IEEE*, volume 4,

pages 1915–1920. IEEE, 2005.

[51] Abedelaziz Mohaisen, YoungJae Maeng, and DaeHun Nyang. On grid-based key pre- distribution: Toward a better connectivity in wireless sensor network. In *Pacific-Asia confer- ence on knowledge discovery and data mining*, pages 527–537. Springer, 2007.

[52] Alok Kumar and Alwyn Roshan Pais. A new hybrid key pre-distribution scheme for wireless sensor networks. *Wireless Networks*, pages 1–15, 2018.

[53] Abedelaziz Mohaisen, Nam-Su Jho, and Dowon Hong. A computationally-efficient construction for the matrix-based key distribution in sensor network. In *International Conference on Infor- mation Security and Assurance*, pages 190–199. Springer, 2009.

[54] Debby Wallner, Eric Harder, and Ryan Agee. Key management for multicast: Issues and ar- chitectures. Technical report, RFC 2627, 1999.

[55] Saurabh Singh, Pradip Kumar Sharma, Seo Yeon Moon, and Jong Hyuk Park. Ad- vanced lightweight encryption algorithms for iot devices: survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–18, 2017.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[56] Panayiotis Kotzanikolaou, Emmanouil Magkos, Dimitrios Vergados, and Michalis Stefanidakis. Secure and practical key establishment for dis- tributed sensor networks. *Security and Commu- nication Networks*, 2(6):595–610, 2009.

[57] Arvinderpal S Wander, Nils Gura, Hans Eberle, Vipul Gupta, and Sheueling Chang Shantz. En- ergy analysis of public-key cryptography for wireless sensor networks. In *Pervasive Comput- ing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*, pages 324–328. IEEE, 2005.

[58] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz. Comparing elliptic curve cryptography and rsa on 8-bit cpus.In *International workshop on cryptographic hardware and embedded systems*, pages 119–132. Springer, 2004.

[59] Gunnar Gaubatz, Jens-Peter Kaps, and Berk Sunar. Public key cryptography in sensor net- works—revisited. In *European Workshop on Se- curity in Ad-Hoc and Sensor Networks*, pages 2–18. Springer, 2004.

[60]S Vijayarani, Ms J Ilamathi, and Ms Nithya. Preprocessing techniques for text mining-an overview. *International Journal of Computer Science & Communication Networks*, 5(1):7–16, 2015.

[61] Haodong Wang, Bo Sheng, Chiu C Tan, and Qun Li. Comparing symmetric-key and public- key based security schemes in sensor networks: A case study of user access control. In *The 28th international conference on distributed comput- ing systems*, pages 11–18. IEEE, 2008.

[62]Shivangi Goyal. A survey on the applications of cryptography. *International Journal of Science and Technology*, 1(3), 2012.

[63]Qikun Zhang, Yong Gan, Lu Liu, Xianmin Wang, Xiangyang Luo, and Yuanzhang Li. An authenticated asymmetric group key agreement based on attribute encryption. *Journal of Network and Computer Applications*, 123:1–10, 2018.

[64]Song Ju. A lightweight key establishment in wireless sensor network based on elliptic curve cryptography. In *Intelligent Control, Automatic Detection and High-End Equipment (ICADE), 2012 IEEE International Conference on*, pages 138–141. IEEE, 2012.

[65]Seung-Hyun Seo, Jongho Won, Salmin Sultana, and Elisa Bertino. Effective key management in dynamic wireless sensor networks. *IEEE Trans- actions on Information Forensics and Security*, 10(2):371–383, 2015.

[66]Chandrasegar Thirumalai and Sathish Shan- mugam. Multi key distribution scheme by dio- phantine form for secure iot communications. In *Power and Advanced Computing Technologies (i- PACT), 2017 Innovations in*, pages 1–5. IEEE, 2017.

[67]QiangHuang,JohnasCukier,Hisashi Kobayashi, Bede Liu,and Jinyun Zhang. Fast authenticated key establishment protocols for self-organizing sensor networks. In *Proceed- ings of the 2nd ACM international conference on Wireless sensor networks and applications*, pages 141–150. ACM, 2003.

[68]Xixiang Lv, Hui Li, and Baocang Wang. Authen- ticated asymmetric group key agreement based on certificateless cryptosystem.*International Journal of Computer Mathematics*, 91(3):447– 460, 2014.

[69]Xixiang Lv, Yi Mu, and Hui Li. Key manage- ment for smart grid based on asymmetric key- wrapping. *International Journal of Computer Mathematics*, 92(3):498–512, 2015.

[70]Dibyendu Chakrabarti, Subhamoy Maitra, and Bimal Roy. A hybrid design of key pre- distribution scheme for wireless sensor networks. In *International Conference on Information Sys- tems Security*, pages 228–238. Springer, 2005.

[71] Hong Lai, Liyin Xue, Mehmet A Orgun, Jinghua Xiao, and Josef Pieprzyk. A hybrid quantum key distribution protocol based on extended unitary operations and fountain codes. *Quantum Infor- mation Processing*, 14(2):697–713, 2015.

[72]R Lalu Naik and P Chenna Reddy. Towards se- cure quantum key distribution protocol for wire- less lans: a hybrid approach. *Quantum Informa- tion Processing*, 14(12):4557–4574, 2015.

[73] Lamia Benazzouz, Mohamed Elhoucine Elhdhili, and Farouk Kamoun. Towards an efficient rep-

utation based hybrid key management architec- ture for ad hoc networks. *Security and Commu-*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

nication Networks, 3(2-3):261–277, 2010.

[74] Jie Huang and Bei Huang. A security key distri- bution scheme based on energy efficiency for hy- brid wireless sensor networks. *Security and Com- munication Networks*, 7(8):1189–1198, 2014.

[75] EA Mary Anita, R Geetha, and E Kannan. A novel hybrid key management scheme for estab- lishing secure communication in wireless sensor networks. *Wireless Personal Communications*, 82(3):1419–1433, 2015.

[76] K Naveen Kumar and Manisha J Nene. Chip-based symmetric and asymmetric key generation in hierarchical wireless sensors networks. In *Inventive Systems and Control (ICISC), 2017 International Conference on*, pages 1–6. IEEE, 2017.

[77] Effie Makri and Yannis C Stamatiou. Determin- istic key pre-distribution schemes for mobile ad- hoc networks based on set systems with limited intersection sizes. In *2006 IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS)*, pages 833–838. IEEE, 2006.

[78] Filippo Gandino, Bartolomeo Montrucchio, and Maurizio Rebaudengo. Key management for static wireless sensor networks with node adding. IEEE Transactions on Industrial Informatics, 10 (2):1133–1143, 2013.

[79] Mohamed-Lamine Messai, Hamida Seba, and Makhlouf Aliouat. A lightweight key management scheme for wireless sensor networks. The Journal of Supercomputing, 71(12):4400–4422, 2015.

[80] E Baburaj et al. Polynomial and multivariate mapping-based triple-key approach for secure key distribution in wireless sensor networks. Computers & Electrical Engineering, 59:274–290, 2017.

[81] Filippo Gandino, Renato Ferrero, and Maurizio Rebaudengo. A key distribution scheme for mobile wireless sensor networks: q-s-composite. IEEE Transactions on Information Forensics and Security, 12(1):34–47, 2016.

[82] [Quazi Mamun and Muhammad Rana. A partial key distribution protocol for wsns in distributed iot applications. In 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pages 248–254. IEEE, 2017.

[83] Fatma Hendaoui, Hamdi Eltaief, and Habib Youssef. A collaborative key management scheme for distributed smart objects. Transactions on Emerging Telecommunications Technologies, 29(6):e3198, 2018.

[84] Alok Kumar and Alwyn Roshan Pais. A new hybrid key pre-distribution scheme for wireless sensor networks. Wireless Networks, 25(3):1185–1199, 2019.