Key Distribution and Management in WSN Security: A State of the Art

Priyanka Ahlawat

Abstract: ***Offering efficient key management scheme (KMS) in WSN faces many challenges that will significantly impact the design and implementation of security protocols for WSN. The goal of KMS is to provide an effective environment in which the sensor node can communicate in a secure manner. It should be able to resolve the issue of generate, allocate the cryptographic keys in WSN in an efficient and effective manner. Hence, the methods for trustworthy allocation and management of these keys are very important for security of WSN. Many KMSs have been developed in recent years. However inherent characteristics of a WSN make incorporating security a great challenge. This paper presents a comprehensive review of current state-of-the-art of KMS designed for WSN security and compare with respect to several evaluation metrics. This paper also investigates the security requirements, goals and challenges of KMS based on existing literature reviews. We also attempt to provide insight in to potential research trends in the area of WSN security and outline the approaches that are likely to play a very important role.***

Keywords: key management, Wireless sensor networks, key distribution, key revocation, rekeying.

I. INTRODUCTION

Wireless sensor network (WSN) is a well disseminated and interconnected network of many tiny wireless nodes, to supervise a system or environment by measuring its physical characteristics such as temperature, pressure, humidity etc. WSN is widely applied in numerous significant applications like defense, medical, and some industrial processing applications [1-2]. This requires sophisticated security solutions which are challenging because of the wireless node connectivity, low power sensors and unattended operation the tiny sensors may become open to various threats. During a physical node capture, attacker may compromise a node to get its stored keys. When a node is compromised, it may lead to compromise of other non-compromised node. WSN security thus, depends on the effective key distribution which should be resistant to attacks. Hence, characterization of the potential attacks in may occur in the WSN becomes very important for a secure network protocol. To set up a secure communication among the tiny sensors, a secret shared key with other neighboring nodes has to be established. Key management scheme (KMS) is very important to provide integrity, confidentiality and authentication of data traffic. KMS is the process to compute the keys, maintain key establishment and the monitoring continuing keying relationships between authorized users [3]. The resistance of a key management sometime may decrease with increase in number of captured nodes, resulting in degraded security of the overall network. It is very important as well critical to provide a robust underlying key distribution to safeguard the network operation with various potential threats. It can only be achieved when the designer has a clear understanding of the potential vulnerabilities that may be exploited by the adversary[4-5]. Node capture is a great concern in sensor network as exposure of secret cryptographic keys may destroy a large proportion of links in a network [6-9]. when a node is physically captured by the adversary, its keying material gets exposed. It can be used to further attack the network [10]. The adversary is assumed to have capability to compromise any node, intercept any wireless communication. In most WSN, there is lack of control with no prior deployment information of sensor nodes [11-12]. Sometimes the nodes are not able to communicate due to physical distance being greater than communication range, node failures, adversarial attack etc.

The paper is ordered as In Sect. 2, challenges, goals and evaluation metrics of different KMSs are presented. Sect. 3 presents classification of KMS in WSN. Adversarial modeling in WSN is given in Sect. 4. Major research issues of key management in WSN security are presented in Sect. 5. Finally, the paper is concluded in Sect. 6.

II. KEY MANAGEMENT IN WSN SECURITY

The tiny sensors are generally not tamper resistant. Thus, an adversary may compromise all the cryptographic keys of a node after physical capturing of a node [1-5, 13, 14]. The sensor nodes are resource constrained and so traditional security mechanism are not feasible for WSN. This is due to increased overhead in the communication and computation of the security mechanism increased on sensor nodes making it as a challenging issue [15, 16]. Because of their large scale and network dynamics, there is no single controlling entity in WSN. Due to their placement in harsh areas, they are susceptible to many attacks [17-21]. The open communication channel also induces various errors, failure of routers, and loss of packets in the network posing difficulty to security mechanism.

KMS uses a set of methods to create, distribute and management the cryptographic keys in sensor nodes. Symmetric cryptography is not computationally efficient and due to frequent rekeying it is difficult to implement it in WSN. The most feasible solution is the key pre-distribution that pre-distributes the keys in to sensor nodes at the time of deployment [9].

Revised Manuscript Received on December 22, 2019.
***** Correspondence Author
Priyanka Ahlawat*, Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India. Email: priyankaahlawat@nitkkr.ac.in

Before discussing them in detail, we firstly discuss the issues, challenges, goals and evaluation metrics of KMS. Key management involves several issues such as the generation of cryptographic keys, storage of keys, life time of the keys, access of the keys, managing the compromise of a key or set of keys [7]. KMS faces many challenges in WSN that will significantly impact the design and implementation of security protocols for WSN [10]. It is the collection of functions and techniques to support the generation, set up and maintenance of the keying associations between legitimate parties [1]. It includes different phases like computation of the secret pair wise keys by key distribution server, their assignment in to the sensor nodes, exchange of key identifiers to set up the pair wise keys, path key establishment with rekeying. KMSs can have symmetric distribution of keys and asymmetric distribution of keys. Symmetric key distribution involved use of similar keys by both communicating nodes for communication. In asymmetric key distribution, communicating nodes use distinct keys. Key distribution server key pre distributes the keys in to the sensor nodes. After their deployment, the communicating nodes creates a shared key to set up a secure communication. KMS are majorly classified in to three types namely- arbitrated schemes, self enforced scheme and schemes with key pre-distribution [5].

After the pair wise keys are set up, the nodes may perform rekeying that may be done periodically so that adversary may not be able retrieve the key. Generally, the changing of keys increases the lifetime of a network with added overhead. The keys can be removed from node key ring when found compromised by attacker and is called key revocation. Key distribution may be static or dynamic. It is based on the rekeying of cryptographic keys is done after the network deployment. KMSs are classified as homogenous and heterogeneous schemes based on role of sensor nodes in the network. Homogenous KMS are used in flat network. Heterogeneous KMS is designed for both flat and clustered network. The keys used by sensor can be of four types namely individual keys, group keys, cluster keys and pair wise keys [22]. Individual keys are shared by the node and base station. Group key is locally shared among a defined group of sensors.

Cluster key is common to a node and its neighboring nodes in a cluster. In pair wise, every node shares at least a single common key with every neighboring node for secure communication. A scheme is not only judged by the capability to offer secrecy of the transferred messages but also to meet definite criteria of efficient in terms of resistance against node capture. During the design any scheme, he network designer should ensure that there should least key leakage when a node is physically captured by the adversary.

Challenges faced by key Management in WSNs

There are various challenges or constraints in WSN that is faced in designing and implementation of an effective security solution for WSN such as key management [2-5]. These are as follows:

a) Lack of defined infrastructure
b) Very large and dense deployment
c) Vulnerability of node to physical capture
d) Vulnerability due to over reliance on BS
e) Lack of prior deployment knowledge
f) Limited memory and computation capacity
g) Impaired wireless channel and limited bandwidth

These challenges induce several constraints in implementing security solutions for such networks.

Goals of KMS in WSN

The main aim of KMS is to resolve the problem of generation, distribution and maintenance of secret keys in an efficient and effective manner. We find the following goals of KMS[4-7]:

a) ***Confidentiality:*** The key management should be able to protect the exchanged data from the attackers. KMS should provide mechanisms to protect the keys so that data cannot be revealed to the adversary.

b) ***Integrity****:* Key management should provide mechanisms to inhibit the entry of unauthorized nodes in the network and only authorized nodes can update the keying material.

c) ***Scalability:*** Key management should provide scalable keys that provide high security not only to small sized networks but also to network with larger number of nodes.

d) **Flexibility:** Key management should be stretchy enough for node addition and able to function well even in intimidating environments.

e) ***Resilience*****:** Key management should be resilient against node capture. If the adversary captures any node, it should prevent the exposure of keys of other non compromised nodes in the network.

f) ***Revocation*****:** If any node is captured then key management should remove the node dynamically from network.

g) ***Resistance against node capture*****:** Key management should resist the addition of cloned nodes by adversary in the network.

Evaluation metrics for KMS in WSN

To evaluate the performance and effectiveness of a particular KMS in WSN security, several metrics are defined in KMS literature [1-7]. These metrics are broadly classified as the security, efficiency and flexibility metrics. Security metrics are required to evaluate the security of the scheme during a node capture attacks or collusion keys, etc.. Efficiency metrics relates with the efficient execution of KMS on the sensor nodes based on the energy, memory, bandwidth. Flexibility deals with mobility support, extensibility, ability to support large networks and key connectivity among sensor nodes. These are explained below:

Security metrics

a) **Node Revocation:** KMS should dynamically remove the misbehaving node from the network. This prevents the compromise of other non compromised nodes during a node capture.

b) **Secrecy of forward and backward communication:** Forward secrecy prevents the node to decrypt the new message with previous key whereas backward secrecy refers to decrypting old messages with new key.

c) It should support both backward and forward secrecy to resist attacks.

d) **Collusion resistance:** Due to random pre distribution of keys, keys stored in compromised nodes may collude with keys stored in non compromised nodes. Thus whole network may be compromised.

e) Resilience against node capture: It is the fraction of the total secure links compromised by capturing n nodes by an attacker [3]. Key management should minimize the key exposure problem.

f) Resilience against node replication: Adversary may introduce clone nodes in a WSN. It may prevent the other legitimate nodes to communicate. Thus, key management should resist against node replication attacks.

Efficiency metric

a) ***Memory footprint/ Storage overhead (SO)* :** It is one of the most important efficiency metric. It is the keying information to be assigned to each sensor node in the network (<4kB of data memory and <48kB of instruction memory). It shows the complexity of the underlying application running in the sensor node. It is significant to identify the exact amount of memory used for storing security credentials of a KMS.

b) ***Bandwidth*:** It refers to the quantity of exchanged messages during the key generation, node eviction and rekeying process in a KMS to determine overall performance of the network.

c) ***Energy*:** The amount of energy consumed during the key establishment of pair-wise security credentials between sensor nodes is also an important metric.

Flexibility metric

a) ***Mobility*:** Most of KMS assume that a node is stationary. However mobility of BS or sensor nodes is required for some applications. Thus, key management should support the mobility of nodes.

b) ***Scalability:*** The sensor nodes are placed in huge quantity in the sensor fields. Thus, KMS should be able to support large sized networks. The protocols should be developed to handle a network of huge number of nodes.

c) ***Extensibility*:** A network should support addition of new nodes after its initial deployment. It becomes very important when they have hostile deployment of external entity.

d) ***Key connectivity*:** It is the probability by which neighboring nodes are connected in a WSN. It is the characteristic that relates with capacity of two sensor nodes to have common security credentials. It is of three types namely global connectivity, local connectivity and node connectivity. The ratio of the largest size of isolated components in network to the size of whole network contributes to global connectivity of sensors. The connectivity among neighboring nodes after shared key discovery phase is over is the local connectivity. The neighboring nodes should ideally communicate without any communication overhead or negotiation. The probability that two nodes share at least one key identifier irrespective of their location in sensor field is the node connectivity. It becomes important when the network survivability of network is great concern in any real time application[3].

III. CLASSIFICATION OF KMS IN WSN SECURITY

A keying relationship can be called as process by which the communicating sensors share a common data (keying material) to implement cryptography techniques [1-3]. It enables the sensors to communicate securely with each other using cryptographc techniques. This data may be a public or secret cryptographic keys, initialization values and some additional non-secret parameter. Typically, the secure communication is achieved either by a sole key shared by all sensor nodes or each sensor nodes will store the set of pair-wise key with other neighboring nodes of the network [4-7]. Both schemes seems infeasible for WSN security. The single wide key is poor against node capture attack as a single node can compromise all the nodes in the network.

The second scheme requires a more keys to be stored in sensor nodes. Moreover, it does not maintain node addition. In arbitrated schemes, a trusted third party will distribute the communication keys to the sensor nodes whenever it is required or asked by the sensors. It makes this scheme less feasible in WSN because the mobile nodes may not be in communication range of distribution centre all the time. Lack of deployment knowledge, dynamic network topology, resource constrained sensor nodes also makes this scheme unsuitable for WSNs. Moreover, if the key distribution centre is compromised, complete network will be compromised making these schemes impractical for WSN applications. It can be further classified as base station participation and trusted third node. In former, BS is the key distribution centre and whenever two nodes wants to communicate, they will send the request for session key to BS (each sensor node share a key with BS).

This scheme has perfect resilience with a drawback that BS should always be in communication range of nodes for session key establishment. in second scheme, a third node (share key with both nodes) may generate the key for communication between the two sensor nodes. Self enforced schemes are based on the asymmetric cryptography that is computationally expensive for WSNs. These are fully distributive and self organized and does not have any trusted third node. The scheme is not robust to variable network topology or to the unreliable links. Moreover, these schemes require that all nodes should be online during the key agreement process. It cannot be satisfied in WSN. Further frequent rekeying in these scheme is troublesome for the sensor nodes. Key predistribution schemes are the most promising solution for WSN because of the indefinite topology prior to the deployment and movable nodes. In these schemes, key distribution centre stores a subset of keys in to sensor nodes from a set of keys at the time of node deployment.

Such schemes seem to be the most appropriate for WSN security.

Although self enforced schemes seems very attractive as

it has trustworthy mechanisms for authentication and key distribution. These schemes greatly suffer from large computation complexity, more memory and high computation overhead. Thus, it is infeasible for WSNs. Therefore, KPS still seems to be the most promising KMS in WSN security. It offer practical and efficient solution to the key management problem in sensor networks. A summary of different KMS is listed in Table 1.

(i) Key predistribution schemes

In this scheme, an offline key server pre-initializes each node with a set of some secret information by which every subset of node find or computes a common key. It is practical solution for those networks where the network topology is unknown. There are two basic schemes for KPS. The first scheme is pair wise key predistribution, every node stores a unique pairwise key with other network nodes but due restricted resources, it is not feasible and has scalability issue. The master key predistribution requires every node to share same symmetric key. It induces no communication, computation overhead and good scalability. But it is not resistant to the node capture attack. Based on the network structure, these schemes are classified as centralized and distributed. The centralized schemes rely on a single entity for key generation and establishment whereas in distributed there is no single entity. Based on the key establishment, the KPS is further classified as:

- Basic scheme
- Shared Key Threshold Random scheme
- Deployment based scheme
- Pair-wise scheme with Structured Pool
- Master key pre-distribution key
- Path Key Establishment
- Rekeying and Key Revocation
- Master key based scheme
- Hybrid schemes
- Attack model based scheme
-

(i) Basic scheme

This was the first scheme proposed by Eschenauer and Gligor [13] known as EG scheme. This scheme is the probabilistic approach for distributed networks. It has three phases namely:

- Key predistribution
- Shared secret key discovery
- Path key establishment

The key distribution server allocates keys with their key identifiers into the sensor nodes before their placement in sensor field. The key ring size is based on the required value of the connectivity in the network. This phase ensures that with small number of keys, the nodes can set up a shared key wit very high probability. During the shared key discovery phase, the nodes start broadcasting their key identifiers to the neighboring nodes in the network. This phase can be secured by a challenge response strategy. In the challenge response the sender nodes builds a challenge for each key in its key ring. When received by the node, it decrypts the challenge only when it has the same key in its key ring. In this way, the neighboring nodes finds their common keys. Thus, this phase establish a secure direct link between the nodes if they share a common key. The neighboring nodes find the shared key by matching the key identifiers. If nodes are not able to find a matched key identifier, they may perform the establishment of a path key. It can be done by selecting some unused key from their key ring. The path key is transferred between the two nodes with the help of intermediate nodes of the network.

This scheme cannot guarantee full connectivity between nodes. The security leakage occurs during the broadcast of the key identifiers in shared key discovery phase. The attacker may analyze the network data through eavesdropping. It can be prevented by generating a random value x by a node encrypted with its own keys and broadcast to other sensor nodes. Any node sharing the common keys with that node can only decrypt the random value x. But this induces overhead on the resource constrained sensor nodes.

The most important issue in this scheme is how to select the right parameters of the key pool size and the key ring size to provide high connectivity in the network. Pietro et al.[23] observed that it is not completely satisfactory as it does not consider the geometric position of the sensors and unable to model the inherent locality of physical visibility. Later, a precise way to choose the value of relevant parameters was also given.

(ii) Shared key threshold scheme

The q-Composite Scheme is based on the shared key threshold approach[14]. The scheme is presented by Chan et al. in 2003. in which the neighboring nodes have at least q common keys to set up a secure link. The process of pair wise key establishment is same as in EG scheme. In order to set up a pair wise key, the neighboring nodes should share q or more than q keys,. They will set up a connection by taking the hash of all matched keys between them. In this scheme key ring size has to be chosen in such a way that network share a expected value of connectivity and resilience against node capture. If key pool is enlarged, the probability of finding common key will decrease. If small key pool size is taken, then network is less secure as adversary can get whole key pool by capturing less number of nodes. Providing a tradeoff between connectivity and resilience is a big challenge in shared key threshold scheme. This scheme has better resilience than EG scheme but scalability is a big issue. Moreover, it does not provide authentication among the nodes.

The key overlap increases the security of the link because the resilience increases with increase in value of q. The attacker has to capture large number of nodes to break that link.

The size of key pool becomes very critical to determine the performance of *q*-composite scheme. With a given key ring size *m*, key overlap *q* and minimum connection probability p_{min}, the largest key pool size is chosen in such a way that $p_{min} < p$. This scheme is better than other schemes in terms of the resilience against the node capture if the number of captured nodes is small. However in large scale attacks, it fails.

(iii) Location aware KMS

This scheme uses deployment knowledge to redistribute the keys in sensors. In many WSN applications, we can approximate the position of sensor nodes. This deployment knowledge can be used to know the possible set of neighbors in a network [13, 24]. This facilitates the network designer to store more keys in neighboring nodes to increase the probability of connectivity. It can be classified as :

- Deployment based random key predistribution scheme-Liu et al. proposed two schemes for WSN using deployment knowledge [25]. The first scheme known as closet scheme that pre-distributes the keys in such a manner that the neighboring nodes share large number of key identifiers than non neighboring sensor nodes. This increases the local connectivity of the network. This scheme performs better if the network designer knows the real location information of the sensor nodes is available to the key server. However, due to memory space, sensor density, communication range, deployment error, its implementation is very difficult in the sensor nodes. The second scheme distributes the polynomials shares to the sensor in order to establish common key. This scheme combines the bi-variate polynomials and location information of the sensors for generating the cryptographic keys. The target field is divided in number of groups /cells. Each cell is associated with unique vicariate polynomial. Each sensor is assigned a polynomial share that belongs to the neighboring cells. An extendible key management scheme is presented by Levi et a. [26] that uses the concept of reusable key pools. First scheme uses two large key pools whereas second scheme use two key pools for each line over a grid based structure. It is shown that proposed schemes have enhanced the security and has good extendible property.
- Group based scheme: Group based KMS are based on two models-node deployment knowledge and a redistribution scheme [27]. If the sensor nodes are to be deployed *i* area, they are divided in to the equal small sized groups. The groups which are deployed closely will share more keys than other ones. The logical distance between the groups of sensor nodes is the inversely proportional to the overlapping of their key identifiers. Different groups are assigned keys from distinct key sub pools. The key pool P is divided into sub key pools with each sub key pool will have *n* keys. In the key predistribution scheme, the key pool is divided in to s*t key pools. while during distributing of the keys, the key pool of the neighboring nodes have more common keys. Deployment model generally follows a grid based approach. This scheme has good storage, connectivity and resilience against node capture but with added complexity. It has less storage, good resilience and connectivity but complex implementation.
- Grid based scheme: Huang et al. proposed a grid based location dependent scheme, the sensors in this scheme have uniform distribution [28]. The sensor field is partitioned in to the small squared sized areas and the sensors deployed in this areas form a group. The scheme uses a polynomial based scheme in which the sensors of the adjacent grid share more polynomials shares than the non adjacent grid. It is resistant to smart node capture attacks and node fabrication attacks. This scheme requires fewer number keys as compare to other schemes.

Pair wise key redistribution scheme with structured pool

The KMS can be further classified as deterministic or probabilistic. In probabilistic scheme, the neighboring may or may not share a common key. In deterministic KMS, a public and private information is stored in the nodes. During establishment of the pairwise key, the nodes exchange their public information and compute the pairwise key. This scheme further classified as: *Deterministic pair wise key predistribution schemes:* Bloom [29] provided the matrix based key distribution. This scheme is perfect pair wise scheme i.e. it has a complete graph. Blom scheme is based on the MDS (Maximum Distance Separable) code. The complete matrix is not broadcasted only id/seed is sent to other neighboring nodes. The sensor nodes can compute the whole matrices. This scheme has perfect connectivity but resilience and scalability are challenges. If λ nodes are compromised, whole network is compromised.

Blundo et.al[12] presented polynomial scheme in which the server selects a bivarate λ degree polynomial which is symmetric where $f(x,y)=\sum_{i,j=0}^{\lambda} a_{ij} x^i y^j$ over GF(q) where *q* is prime number and is the range of cryptographic keys. Each node is loaded offline with its polynomial share. Node S_a, a polynomial share f(a,y) is calculated and stored. After deployment, the common key K_{ab} is computed by S_a and S_b i.e. f(a,b) is computed as polynomial is symmetric, both sides compute the same secret key. The storage overhead is $(\lambda+1)\log_2 q$ with no communication overhead.

Combinatorial based scheme: In this scheme, key distribution is based on partially balanced incomplete block design. It is shown that it has better network resilience and scalability in WSN [30].

Non deterministic KMSs-Du et. al scheme: This scheme provides the enhancement of the security in Blom [27]. Du et al. solution also called as Multiple-Space Key Pre Distribution Scheme. It consists of three phases i) key redistribution phase ii) key agreement phase iii) key agreement phase. In key predistribution phase, a matrix G is generated of size (λ+1) ×N and node *i* will be assigned G(I) where i^{th} column of matrix G. A second matrix D is generated (symmetric) of size ((λ+1)((λ+1).then distinct key spaces are selected from a pool for each node. In key agreement phase, each node needs to discover whether it shares any key space with its neighbors. If the key spaces are not shared, then key is established with help of the neighboring nodes.

This scheme has good resistance against attacks. It has communication overhead (in case of path key establishment phase) is a challenge. Scalability is also an issue in this scheme.

Liu and Ning scheme [31] is the polynomial based key management.

This scheme is introduced by Liu and Ning. Polynomial has the property that f(x,y) = f(y,x). if nodes *i* and *j* receive polynomial f(i,y) and f(i,x) respectively can compute the common key. In this scheme, a pool of randomly generated polynomial are used to establish a pair wise key between the nodes. The setup phase stores the polynomial shares in sensors. After deployment, if two sensors want to establish communication, they do so by direct key establishment phase. During a shared key phase, the sensors nodes may not be able to find a common key due to random key distribution, they perform path key establishment phase. Based on above framework, two instantiations are proposed namely random subset assignment and grid based key redistribution scheme. In random subset assignment, the node share IDs of other nodes with whom it share polynomial share. In random election of polynomial pools, node are stored with polynomial share. In first phase, they broadcast polynomial IDs and other nodes with which IDs match, can establish link. The nodes which do not share polynomial share can communicate through path key establishment phase. If one communication link is compromised other link may be compromised having same polynomial share. In grid based scheme, there is no broadcast of IDs, thus no communication overhead. In this scheme, whole network is compromised if more than λ-nodes are compromised. Polynomial based key pre-distribution scheme has reduced pre-distributed information of keys.

(iv) Hashed key predistribution

In order the increase the security of the KMS, one way hash functions are used on the pre-distributed keys of the sensor nodes at the time of deployment in sensor field. The keys are thus concealed and their disclosure only reveal the derived versions of the key to the adversary. These schemes induce some computation overhead. In 2013, Bechkit et al. applied hashing on the keys. The number of hash is based on their node identifiers value. It increases resilience against node capture of resulting key predistribution scheme [32]. Two improvements are given in [33] by Kur et al. First scheme exploits the limited key collisions in secure hash functions to increase the probability of connectivity. The second scheme uses hash chain on key pool to increase the resilience against node capture. An improved scheme based on bidirectional hash chains is presented by Dalai et al. in [34]. In this scheme, bidirectional hash chains are mapped with q-composite scheme.

(v) Predistribution with multiple sub key pools

A dual key pool scheme uses different key pools for different types of communication. It results in improved resilience against node capture. It also has reduced communication overhead [35-37]. In [35], authors applied the concept of dual key sub pools for distributing the keys. It further reduces the communication overhead of the scheme. The size of the original key pool is increased by applying hash computation and random numbers followed by integrating with original key pool. This method improves the key connectivity. It also increases the resistance of distribution scheme. A two level key pool is presented by Mohaisen et al., in 2010. This scheme splits the original key pool into different sub key pools [36]. This also results in reduced communication overhead. A deployment based KMS is proposed in [38] to make WSN more resistant against physical node capture. Cell of the network are assigned different key ring sizes to increase the security of the scheme. To reduce the communication overhead, the key pool is partitioned.

(vi) Path Key Establishment

Chan et al. proposed path key establishment scheme for WSN that states that if neighboring nodes are not able to find any common key, they can establish the key with the help of intermediate nodes [22]. This scheme uses multiple disjoint paths. These paths are used to transfer the path key from a source to destination node [39-42]. The secrecy of the path key depends on the security of reliability of underlying paths. This scheme is used in conjunction with random key predistribution scheme to strengthen the security of communication link [43]. As the keys are randomly distributed among the sensor nodes (more chances of repletion of keys), capturing of any node by adversary may reveal the communication key of other node. Thus, we establish the link key from multiple paths between the communicating nodes [43]. Whenever nodes wants to communicate, they update the communication key with some random value. This scheme has better resilience than EG scheme but communication overhead for new link key establishment is more. The scheme is simple to implement, efficient and scalable than full pair-wise key management scheme. Node authentication is again not supported in path key establishment. Table 1 gives a comparative anlysis of different schemes.

S.No.	KMS	Security	Sc	Connectivity	SO	advantages	disadvantages	mobility	distributed
1	Master key	Master key compromise leads to complete disruption of network	Very high as network uses single key	Very high as all nodes uses same key	Very low	Self organizing Lower key set up time Efficient in terms of time	Low resistance against node capture	No	no
2	Probabilistic based scheme:	Keys assigned to nodes	medium	Depends on key pool and key ring	Generally high	Easy to implement	Large memory requirement difficult rekeying and key revocation	no	no

3	q-composite scheme	High for small networks	low	Low than basic scheme	Same as in basic scheme	High security	Connectivity decreased due to more required key overlap	no	no
4	Polynomial scheme	thigh	high	high	high	High scalable High connectivity	Large memory overhead and threshold property	no	no
5	Matrix scheme	thigh	high	high	high	High connectivity	Large memory overhead and threshold property	no	no
6	group based scheme	Log_2n	Low	high	low	Low time delay	Computation overhead	no	no
7	Deployment based schemes	high	Medium	high	low	Neighboring nodes share more keys	How to guess exact location before deployment is difficult	no	yes
8	Key splitting based schemes	high	Same as in basic scheme	high	low	Increased security against node capture , attacker has to capture large number of nodes to get the complete key	Increased computation	no	no
9	Unbalanced key distribution	high	Medium	Same as in basic scheme	Decreased on low end nodes	Decreases the complexity of low end nodes	More suitable for heterogeneous networks	Yes(incase low end nodes are mobile)	yes
10	Hashed key distribution	Very high	medium	Same as in basic scheme	high	Increased security	Hash function increases computation complexity	No (depends if sink is mobile)	no
11	KMS with key deletion	Very high	low	Low	low	Increased security against node capture	Effects key connectivity	no	no
12	Multiple sub key pools	high	low	medium	low	Low overhead during shared key establishment	Randomness of keys assigned from sub key pools decides performance	no	no
13	Hybrid schemes	Very high	medium	medium	medium	Aims to increase security of kms	Increased complexity	no	no
14	Attack resistant schemes	Very high	medium	high	medium	Predistribution of keys according to adversarial behavior, thus generally have high resistance against node capture	Performance is based on how efficient is adversarial pattern	no	yes
15	GA based KMS	high	high	high	low	Depends on sharing of key slices	Increased processing cost	no	yes

(vii) Key splitting based scheme

To improve the resilience of key management, a key splitting method is presented by Ehdaie in [44]. In this scheme, keys in pool are divided in to *z* equal parts thereby increasing the size of key pool. This results in less key exposure during a node capture. A comparative analysis of different path key establishment scheme is given in Table 2.

Table 2: Path key establishment schemes in WSN

Scheme	Technique	Advantages	Disadvantages
[Li et al. 2006]	Proxy based scheme	Resistant to node capture attacks, utilizes keying information	Hard to find proxies
[Gupta et al. 2006]	Friend based scheme	Less resistant than proxy based , utilizes keying information	More efficient than disjoint path based
[Ghafoor et al. 2016] [Hayajneh et al. 2014]	Disjoint path scheme	Paths are selected to transmit the key fragments	Routing information is required

(viii) Rekeying and Key Revocation

WSN is highly vulnerable to attacks because they consist of numerous small resource constrained nodes that interact closely with environments. This makes the scheme less resistant to node capture. In order to improve the security, the link keys have to rekeyed to maintain the secrecy and resiliency against such attacks. The survivability of KMS against attacks is a challenge in WSN[45]. Based on the capability of the cryptographic key updating during run time, these schemes can be classified as static and dynamic. In static scheme, once the keys are assigned to sensor nodes by key server, it will not change. The exclusion of BS in KMS is one of the advantage of this scheme. However, prolonged use of cryptographic keys may leads to increase in probability of being attacked. This leads to dynamic key management that advocates the change of keys to provide attack resiliency. In this rekeying, keys are assigned multiple times to the sensor nodes. In static rekeying, there is no change in session keys in as the keys are generated once at the time of deployment. The most important concern is that a key is lost when compromised by the adversary during node capture[22]. In dynamic KMS revealed keys are modified to prevent further attacks in the network. Thus, it is regarded as the most promising approach in sensor networks as it increases the network survivability and the network resiliency. A adversarial model based rekeying approach is given in [46]. It is based on the backup link key which reduces the communication and computation overhead of the proposed scheme. A time variant rekeying is given in [47] that aims to make the network more secure. A summary of rekeying schemes is given in Table 3.

Table 3: Rekeying schemes in WSN

Scheme	Technique	strength	weakness
[Eschenauer'02]	1 to N	Compromised key is revoked from non compromised nodes	Large communication overhead Reconfiguration of shared key discovery Normal data communication is interrupted
[Biswas'09]	Fast rekeying	Frequently used key is given higher rank and is ignored during shared key discovery Key with Lower rank is the backup key Number of messages during rekeying are reduced, thus communication overhead is reduced	Security is not considered

Master key based schemes: In this scheme, a single key is stored in each sensor node. It has perfect connectivity, less storage requirement but with low resilience against node capture [3]. There is no key discovery or key exchange in this scheme. After deployment every node uses the identical key for encryption and decryption of messages.

(ix) Hybrid schemes

Two or more than two schemes with different functionalities are combined together to form a hybrid scheme. A key establishment presented by Zhang et al.[48] that combines polynomial pool based key distribution and probabilistic KMS. The polynomial shares are given to the sensor nodes to form a key pool. The nodes are assigned keys from that key pool. This scheme has higher resilience against node capture. A scheme known as PPBR that merges polynomial and random key predistribution is presented by Zhang et al. in [49]. It has less storage and more resilience against node capture. Anita et al. [50] merged the polynomial pool scheme with *q*-composite scheme to decrease the impact of compromised key on other nodes. A scheme is given in [51] that combines the q-composite scheme with polynomial scheme that uses hash functions to increase the resilience against node capture.

(x) Attack model based scheme

In this key predistribution, attacker behavior is used to predistribution the keys among the sensor nodes. A application based key predistribution was given by Yu et al. in [52] to store the keys based on the application or network traffc flowing in the nodes. The nodes share more keys in different cells will share more keys if they have larger attack values. This is done in order to enable them to continue processing even if large number of nodes are compromised. In [53], a hybrid path vulnerability matrix based scheme is proposed. it aims to increase the resilience of the network by incorporating attacking behavior of the adversary. It is shown that to maintain same connectivity, the proposed scheme requires lesser key ring size. A dominance rank based KMS is proposed in [54] that consider the key compromise probability to increase the security of resulting scheme.

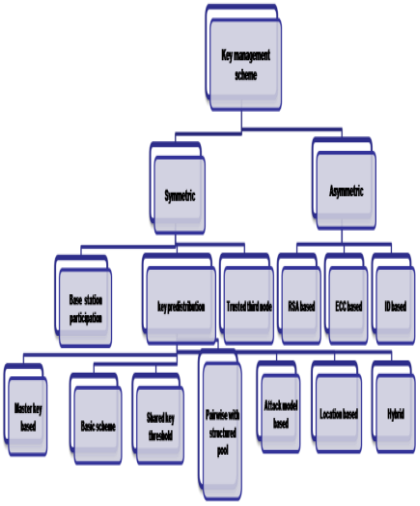

Figure 1: Classification of key management schemes in WSN

IV. RESULTS AND DISCUSSIONS

These sections details the major research issues in field of key management and are as follows:

a) How to design key management solutions for multiphase phase WSN is an open issue. This requires that solutions should be scalable and should support new addition of nodes. Forward and backward secrecy is important issue to consider in multi phase key distribution.

b) In a WSN, the nodes may shift from their original positions after their deployment that means their topology is dynamic. KMS should be designed in such a manner that it should support dynamic behavior. How to maintain required key connectivity levels in such dynamic behavior is also an important issue.

c) Node authentication is also a major issue.

d) How to remove the keys from the non compromised nodes when a node is captured by adversary is also important issue. How to reduce the number of effected nodes during a key revocation is also need to be addressed. It should be lightweight so that it can practically implemented on tiny sensors. Key revocation completely degrades the network. when it should be revoked is also urgent attention on key management research

e) How to provide efficient security as well as connectivity is very important and it needs great attention when designing a key management solution. It entirely depends on applications for which KMS is developed.

f) Rekeying process need to be efficient. How to reduce the number of sensors during a rekeying is also need to be addressed. How to make it more secure is an open issue.

g) Node capture detection should be done immediately. how to devise such methods for WSN is also an open research problem

h) How to design KMS the can work with degraded performance during anode compromise is also need attention.

i) How to select different parameters to evaluate performance of different KMS suitable for real time applications is an open research problem

j) How to find exact and accurate locations of sensors is also an important issue. Some applications have very uneven deployments.

k) Key update period should be critical factor in he overall performance of network. It should be very high with low overhead

l) To optimize different polynomial and matrix based schemes and how to optimize their threshold property also need to be addressed.

m) No key management solutions fits for all applications. Designing such general solution si also an open issue.

n) More research is needed to study the security level of different public schemes applicable to different environment of WSNs

V. CONCLUSION

In this paper, a brief introduction about the design challenges, attacks and security requirements in WSN is presented. It also presents salient features and challenges in implementing KMS in WSN. In this paper, a comprehensive survey of all proposed key management solutions for WSN is presented. The current limitations of the proposed solutions are briefly outlined with discussion on the current challenges that still need further research. We find that a large number of KMS is proposed for WSN security. It is clear that numerous tradeoff exist for different KMS and one must select tradeoff carefully when selecting KMS. It is the basis of secure communication among sensor nodes. Thus, it need greater attention. Development of an efficient KMS for resource constrained sensors is a still remains an open issue. The paper aims to encourage more feasible key management solutions that can be easily mapped to real life applications. It also provides insight so that future KMS can be proposed with increased functionality.

REFERENCES

1. He, X., Neidermeier, M., & Meer, H. (2013). Dynamic key management in wireless sensor network: A survey. Journal of Network and Computer Applications, 36, 612–622.
2. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. Computer Networks, 38(4), 393–422.
3. Zhang, J., & Varadharajan, V. (2010). Wireless sensor network key management survey and taxonomy. Journal of Network and Computer Applications, 33(2), 63–75.

4. Xiao, Y., Rayi, V. K., Sun, B., Du, X., Hu, F., & Galloway, M. (2007). A survey of key management schemes in wireless sensor networks. *Computer communications*, *30*(11-12), 2314-2341.
5. Simplício Jr, M. A., Barreto, P. S., Margi, C. B., & Carvalho, T. C. (2010). A survey on key management mechanisms for distributed wireless sensor networks. *Computer networks*, *54*(15), 2591-26
6. Sun, D., & He, B. (2006). Review of key management mechanisms in wireless sensor networks. *Acta Automatica Sinica*, *32*(6), 900.
7. Lee, J. C., Leung, V. C., Wong, K. H., Cao, J., & Chan, H. C. (2007). Key management issues in wireless sensor networks: current proposals and future developments. *IEEE Wireless Communications*, *14*(5).
8. Camtepe, S. A., & Yener, B. (2005). Key distribution mechanisms for wireless sensor networks: a survey. *Rensselaer Polytechnic Institute, Troy, New York, Technical Report*, 05-07.
9. Nabavi, S. R., & Mousavi, S. M. (2018). A review of distributed dynamic key management schemes in wireless sensor networks. *Journal of Computers*, *13*(1), 77-90.
10. Bhushan, B., & Sahoo, G. (2018). Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks. *Wireless Personal Communications*, *98*(2), 2037-2077.
11. Blundo, C., De Santis, A., Herzberg, A., Kutten, S., Vaccaro, U., & Yung, M. (1992, August). Perfectly-secure key distribution for dynamic conferences. In *Annual International Cryptology Conference* (pp. 471-486). Springer, Berlin, Heidelberg.
12. Du, W., Deng, J., Han, Y. S., Varshney, P. K., Katz, J., & Khalili, A. (2005). A pairwise key predistribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, *8*(2), 228-258.
13. Chan, H., Perrig, A., & Song, D. (2003). Random key predistribution schemes for sensor networks. In Proceedings of 2003 IEEE Symposium on Security and Privacy, California, USA (pp. 197–213).
14. C. Zhu et al. 2015, E. M., Geetha, R., & Kannan, E. (2015). A novel hybrid key management scheme for establishing secure communication in wireless sensor networks. Wireless Personal Communications, 82(3),1419–1433.
15. Gupta, B., & Pandey, J. (2015). Non existence of isolated nodes in secure wireless sensor networks. Wireless Personal Communications. doi:10.1007/s11277-015-2845-9.
16. Chan, K., & Fekri, F. (2011). Node compromise attacks and network connectivity. Proceedings of SPIE, 6578, 1–12.
17. Chen, X., Makki, K., Yen, K., & Pissinou, N. (2007). Attack distribution modeling and its applications in sensor network security. EURASIP Journal on Wireless Communications and Networking, 2008, 1–11.
18. Di Pietro, R., Mancini, L. V., & Mei, A. (2003, October). Random key-assignment for secure wireless sensor networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks* (pp. 62-71). ACM.
19. Yu, C.-M., Li, C.-C., Lu, C.-S., & Kuo, S.-Y. (2011). An application driven attack probability based deterministic pair-wise key predistribution scheme for non uniformly deployed sensor networks. International Journal of Sensor Networks, 9(2), 89–106.
20. Du, W., Deng, J., Han, Y., Chen, S., & Varshney, P. K. (2004). A key management scheme for wireless sensor networks using deployment knowledge. In Proceedings of IEEE INFOCOM'04 (pp. 586–597).
21. Bechkit, W., Challal, Y., & Bouadallah, A. (2013). A new class of hash chain based key predistribution scheme for WSN. Computer Communications, 36, 243–255.
22. Shukla, P. K., Goyal, S., Wadhvani, R., Rizvi, M. A., Sharma, P., & Tantubay, N. (2015). Finding robust assailant using optimization functions (FiRAO-PG) in wireless sensor network. Mathematical Problems in Engineering, 2015, 7 Article Id 594345.
23. Kalkan, K., Yilmaz, S., Yilmaz, O. Z., & Levi, A. (2009, October). 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* (pp. 29-36). ACM.
24. Das, A. K. (2011). An efficient random key distribution scheme for large-scale distributed sensor networks. *Security and Communication Networks*, *4*(2), 162-180.
25. Yu, W. (2010, March). A Pair wise Key Management Scheme Based on Hash Function for Wireless Sensor Networks. In *Education Technology and Computer Science (ETCS), 2010 Second International Workshop on* (Vol. 2, pp. 198-201). IEEE.
26. Levi, A., Taşçı, S. E., Lee, Y. J., Lee, Y. J., Bayramoğlu, E., & Ergun, M. (2010). Simple, extensible and flexible random key predistribution schemes for wireless sensor networks using reusable key pools. *Journal of Intelligent Manufacturing*, *21*(5), 635-645.
27. Kavitha, T., & Sridharan, D. (2013). Probabilistic key chain based key distribution schemes for WSN. *International Review on Computers and Software (IRECOS)*, *8*(5), 1156-1169.
28. Eschenauer, L., & Gligor, V. (2002). A key-management scheme for distributed sensor networks. In Proceedings of 9th ACM Conference on Computer and Communications Security (pp. 41–47).
29. Huang, D., Mehta, M., Medhi, D., & Harn, L. (2004, October). Location-aware key management scheme for wireless sensor networks. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks* (pp. 29-42). ACM.
30. sECURITY IN SENSOR NNETWORKS BOOK
31. Zhang, J., & Ding, Y. (2010, July). Pair wise Key Management Scheme Using Sub Key Pool for Wireless Sensor Networks. In *Information Technology and Computer Science (ITCS), 2010 Second International Conference on* (pp. 21-24). IEEE.
32. Zhang, J., Li, J., & Liu, X. (2009, January). An Improved Pair wise Key Management Scheme for Wireless Sensor Networks. In *Computer Network and Multimedia Technology, 2009. CNMT 2009. International Symposium on* (pp. 1-4). IEEE.
33. Y. Lin, Y. Younan, Y. Wangke, W. Qiuhua, "A key distribution scheme for WSN based on hash chains and deployment knowledge," *Int. J. of Distributed Sensor networks*, vol. 2015, Article ID: 640792, 12 pages, 2015.Dalai,
34. D. K., & Sarkar, P. (2017, August). Enhancing Resilience of KPS Using Bidirectional Hash Chains and Application on Sensornet. In *International Conference on Network and System Security* (pp. 683-693). Springer, Cham.
35. Ergun, M., Levi, A., & Savas, E. (2010). Increasing resiliency in multi-phase wireless sensor networks: generation wise key predistribution approach. *The Computer Journal*, *54*(4), 602-616.
36. Wenqi Yu. A pairwise key management scheme based on hash function for wireless sensor networks, IEEE Second inter. Workshop on education technology and computer science, 2010
37. Kůr, J., Matyáš, V., Švenda, P. (2012, September). Two improvements of random key predistribution for wireless sensor networks. In *International Conference on Security and Privacy in Communication Systems* (pp. 61-75). Springer Berlin Heidelberg.
38. Ahlawat, P., & Dave, M. (2018). Deployment Based Attack Resistant Key Distribution with Non Overlapping Key Pools in WSN. *Wireless Personal Communications*, *99*(4), 1541-1568.
39. Lin, C., Qiu, T., Obaidat, M. S., Yu, C. W., Yao, L., Wu, G. (2016). MREA: a minimum resource expenditure node capture attack in wireless sensor networks. *Security and Communication Networks*.
40. Zhang, Y., Liang, J., Zheng, B., & Chen, W. (2016). A hybrid key management scheme for WSNs based on PPBR and a tree based path key establishment methods. Sensors, 16, 509. doi:10.3390/s16040509.
41. Zhang, J., Cui, Q. and Yang, R., (2016) A hybrid establishment scheme for wireless sensor networks. International Journal of Security and its applications, vol. 10, pp. 411-422.
42. Gandino, F., Ferrero, R., Rebaudengo, M. (2017). A Key Distribution Scheme for Mobile Wireless Sensor Networks: *q*- s-Composite. *IEEE Transactions on Information Forensics and Security*, *12*(1), 34-47.
43. Choi, J., Bang, J., Kim, L., Ahn, M., Kwon, T. (2017). Location-based key management strong against insider threats in wireless sensor networks. *IEEE Systems Journal*, *11*(2), 494-502.
44. Ehdaie, M., Alexiou, N., Attari, M. A., Aref, M. R., & Papadimitratos, P. (2015). Key splitting: making random key distribution schemes resistant against node capture. *Security and Communication Networks*, *8*(3), 431-445.
45. Biswas, S., Haque, M. M., Rashwand, S., Misic, J. (2009, June). Fast, seamless rekeying in wireless sensor networks. In *Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09. 29th IEEE International Conference on* (pp. 166-171). IEEE.
46. Ahlawat, P., & Dave, M. (2017, July). A resilient and seamless rekeying scheme based on random key distribution for WSN. In *Computer, Communications and Electronics (Comptelix), 2017 International Conference on* (pp. 321-327). IEEE.
47. Ahlawat, P., & Dave, M. (2018). An attack model based highly secure key management scheme for wireless sensor networks. *Procedia Computer Science*, *125*, 201-207.

48. Li, G., Ling, H., Znati, T., Wu, W. (2006). A robust on-demand path-key establishment framework via random key predistribution for wireless sensor networks. *EURASIP Journal on wireless Communications and Networking*, *2006*(1), 1-10.
49. Devanagavi, G. D., Nalini, N., Biradar, R. C. (2016). Secured routing in wireless sensor networks using fault-free and trusted nodes. *International Journal of Communication Systems*, *29*(1), 170-193.
50. Bajestani, M. F., Payandeh, A. (2016). A novel key distribution scheme against storage-bounded adversaries using attack probabilities. *Turkish Journal of Electrical Engineering & Computer Scie* Xiong *nces*, *24*(3), 1014-1021.
51. Ahlawat, P., & Dave, M. (2018). An attack resistant key predistribution scheme for wireless sensor networks. *Journal of King Saud University-Computer and Information Sciences*.
52. Kendall, E., Kendall, M., & Kendall, W. S. (2012). A Generalised Formula for Calculating the Resilience of Random Key Predistribution Schemes. *IACR Cryptology ePrint Archive*, *2012*, 426.
53. Ahlawat, P., & Dave, M. (2017). A hybrid approach for path vulnerability matrix on random key predistribution for wireless sensor networks. *Wireless Personal Communications*, *94*(4), 3327-3353.
54. Ahlawat, P., & Dave, M. (2018). A cost-effective attack matrix based key management scheme with dominance key set for wireless sensor network security. *International Journal of Communication Systems*, e3713.

AUTHORS PROFILE

Priyanka Ahlawat, Department of Computer Engineering, National Institute of Technology, Kurukshetra , Haryana, India. Her current research interest includes Information Security, Computer Networks, Internet of Things, Wireless Sensor Networks, Information Security, Cyber Security, IoT Security, Adhoc Network Security, WSN Security, Key Management and Distribution