IWNEST PUBLISHER

Journal of Industrial Engineering Research

(ISSN: 2077-4559)

Journal home page: http://www.iwnest.com/AACE/

Secure Information Transmission and Retrieval Using Key Management in Wireless Sensor Network

Blessey. P.M., Princy, P.M. and Divya, P.

[1]*PG Scholar, Department of CSE, S. A. Engineering College, Chennai.*
[2]*UG Scholar, Department of CSE, Bhajarang Engineering College, Chennai.*
[3]*PG Scholar, Department of CSE, S. A. Engineering College, Chennai.*

ARTICLE INFO

Article history:
Received 23 March 2014
Accepted 24 April 2015
Available online 28 April 2015

Keywords:
Sensor networks, Security, Connectivity Key management schemes, Secure communication.

ABSTRACT

Wireless sensor networks (WSNs) distribute nodes with the limited capabilities to sense, collect, and distribute information in numerous applications [1]. As sensor networks become pervasive, security is exposed to several attacks such as Sybil attack, network eavesdropping, masquerade attack, etc. For secure communication between the nodes, secret key cryptosystem is used. To deliver data in a secure manner without being compromised by an adversary, WSN provides secure communication and key distribution. Key management schemes have been established to achieve security. The tradeoff between the security and the connectivity is explained in each key management scheme. By this survey, it helps us to know the schemes that detect attacks and prevent it. As we recuperate the merits and demerits of the schemes are analyzed. Moreover, the techniques and methods used have been summarized.

To Cite This Article: Blessey. P.M., Princy, P.M. and Divya, P., Secure Information Transmission and Retrieval Using Key Management in Wireless Sensor Network. **J. Ind. Eng. Res.,** *1(4), 69-78, 2015*

INTRODUCTION

Following the recent advances in wireless sensor network (WSNs) has been implemented in various fields such as industry, military, habitat, monitoring and surveillances for sensing, computation and the communication purposes. To provide integrity, authentication and confidentiality in the network, key management schemes with and without the deployment knowledge have been developed. Securing links between the nodes in the network is the main role of the key management schemes [2]. Because of the resource limitation and less computation usage, Symmetric key establishment is the suitable cryptography for secure transmissions in WSNs, where two nodes share a common key for encryption and decryption. Symmetric key cryptography is considered valuable because it is relatively inexpensive to produce a strong key for these ciphers, the keys tend to be much smaller for the level of protection they afford and the algorithms are relatively inexpensive to process. Types of Symmetric key ciphers are stream ciphers and block ciphers [3]. A stream cipher is a method that encrypts the bytes of a message, one bit at a time. Block cipher is a method that encrypts a number of bits as a single unit rather than one bit at a time. Many different approaches have been proposed to manage the keys in WSNs. This includes dealing with the exchange, storage, and usage of keys to provide robustness in the network. These schemes are used to perform cryptographic operations, which are the combination of key and key management function. Various key management schemes and its limitations have been explained in the following:

• Plain global key, where the same key is used by all of the nodes.
• Fully pair-wise keys, where each node has a specific key for every other node, so each possible link has its own key.
• Transitory master key, where each pair of nodes uses a master key as a common secret, to protect the generation of the pair-wise key.
• Random key pre-distribution that assigns a set of k- random keys to each node from a pool of keys.
• Multi-space pair-wise key scheme, pair-wise keys is computed when two nodes have at least one common key space

Corresponding Author: Blessey, P.M., PG Scholar, Department of CSE, S.A. Engineering College, Chennai.
E-mail: blessey.pm@gmail.com

• Q-composite key pre-distribution, where two nodes compute a pair-wise key if they share at least q common keys
• Random pair-wise key pre-distribution randomly picks a pair of sensors and assigns each pair a unique random key.
• Multipath key reinforcement scheme provides security in the links through the common keys in the various node's key rings.
• Random key pre-distribution with transitory master key, two nodes perform a shared-key discovery and it iterates the transformation using the master key which provides keys for communication.
• Random seed distribution with transitory master key, transform shared seed with permutation factor to generate seed which in turn executes with the master key to generate a pair-wise key.

II. Background:

A. Security Goals and Operational Requirements:

Security services in WSNs mainly deal with the protection or defense services against attacks, interference and espionage [1, 3].

 Confidentiality: Confidentiality forces information inaccessible or restrictions to unauthorized user, confidential information is prevented from revealing to any kind of attack.
 Availability: Availability guarantees network services to legitimate user whenever required, by avoiding the denial-of-service attacks that interrupts the services of a host connected to the internet.
 Integrity: Integrity avoids the alteration of data which produce an unauthorized effect.
 Authentication: Authentication confirms that the identity of nodes with which communication takes place.
 Non-repudiation: Non-repudiation guarantees that the sender or receiver of the message cannot deny having sent or received the message.
 Authorization: Authorization specifies the access rights of legitimate nodes to resources or network service.
 Robustness: Robustness ensures that the entire network is not compromised even though fewer nodes are compromised.
 Data Freshness: Always prefers data that is still not used.
 Self-organization: Nodes should be flexible enough to self-organize and self-healing.
 Scalability: Scalability guarantees tosupport number of nodes even with key management in place.

B. Security Challenges:

The security challenges are summarized from [1] as follows:
Minimize power or resource consumption and maximize the security performance.
 Providing the connectivity without any limitation in the resilience.
 Preventing the insider attacks.
 The large scale of the network and the mobility of nodes should not degrade the security performance.

C. Comparison:

The keying models are used to compare the differences in relationships between security and the operational requirements in WSN.
 Network Keying: Network Keying is simple, scalable and flexible, which allows data aggregation and fusion. It can self-organize, but lacks robustness.
 Pair-wise Keying: Pair-wise keying provides best robustness against compromised node and also provides authentication for each node, but it is unable to organize nodes itself and lacks in flexibility and scalability.
 Group Keying: Group keying provides better robustness than network keying. It allows multicast and can also self-organize within the cluster. Here cluster formation is application dependent.

D. Attacks, Vulnerabilities and Threats:

An attack is an assault on system security that drives from an intelligent threat. Vulnerability is a weakness which allows an attacker to reduce a system's information assurance. A threat is a possible danger that might exploit vulnerability. The need for security arises only when there is attack in the network [3]. Generally, the probability of attack within sensor networks is larger. These attacks that compromise the security of the information owned by an authorized party can be classified as internal attacks and external attacks. The internal attack occurs when an individual or a group within an organization seeks to disrupt operations or exploit organization. External attacks are performed by individuals who are external to the target network or organization. External threats are executed by using a predefined plan and the skills of the attacker. The main characteristics of external threats are that they usually involve scanning and gathering information. External attacks can further be divided into two categories: passive and active. Passive attack attempts to make use of information that is being transmitted from the system but does not affect system resources. An active attack attempts to alter system resources or the creation of false data. Some of active attacks are masquerading,

modification of the message and denial-of-service (DoS) attacks [3]. In order to detect, prevent or recover from these security attacks, a security mechanism is designed which is termed as key management schemes.

III. Related Work:

Various key management schemes have been proposed [2] for security purpose. This section describes the techniques used with their benefits and drawbacks.

A. Single Network Wide Key:

This is the simplest scheme that uses a same key used by every node in the network. This key provides a secure communication by employing encryption and decryption operation. The main advantage is that the hardware overhead is limited. Single network wide key doesn't guarantee security since if a single node is compromised, then the whole network is eavesdropped by the adversary. It is the weak scheme against cryptanalytic attacks, but it provides better connectivity.

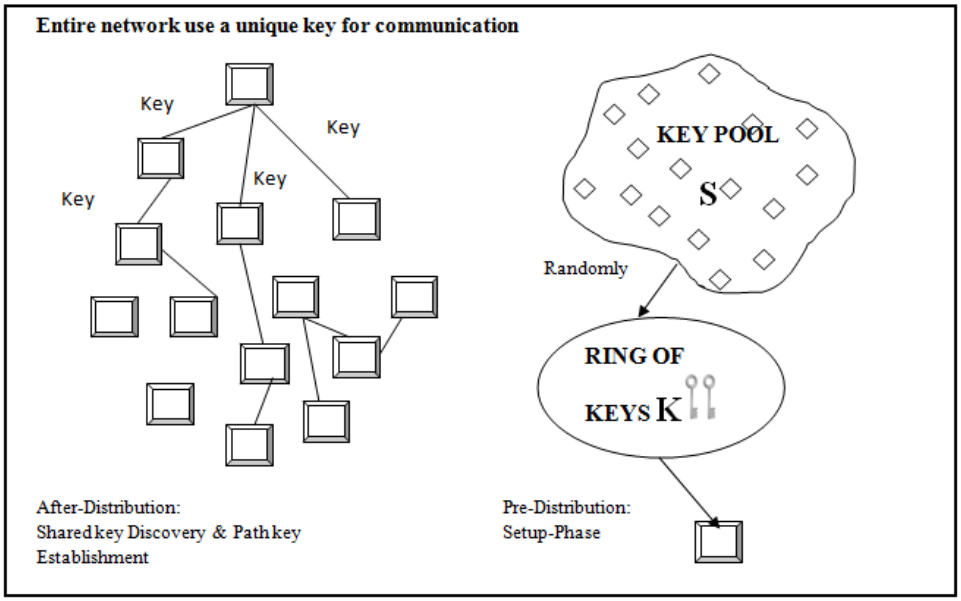

Fig. 1.1: Single Network Wide Key.

B. Pair-wise Key Establishment:

In the pair-wise key scheme, each node has a unique key for every other node in the network for communication. For every authentication between nodes, a specific key is used by one link and the node replication has been limited. This scheme is more secure than a single network wide key, since compromising of a key can eavesdrop only one possible link. The drawback of this scheme is that it uses large memory area to store the keys used in the large network. It provides connectivity same as single network wide key.

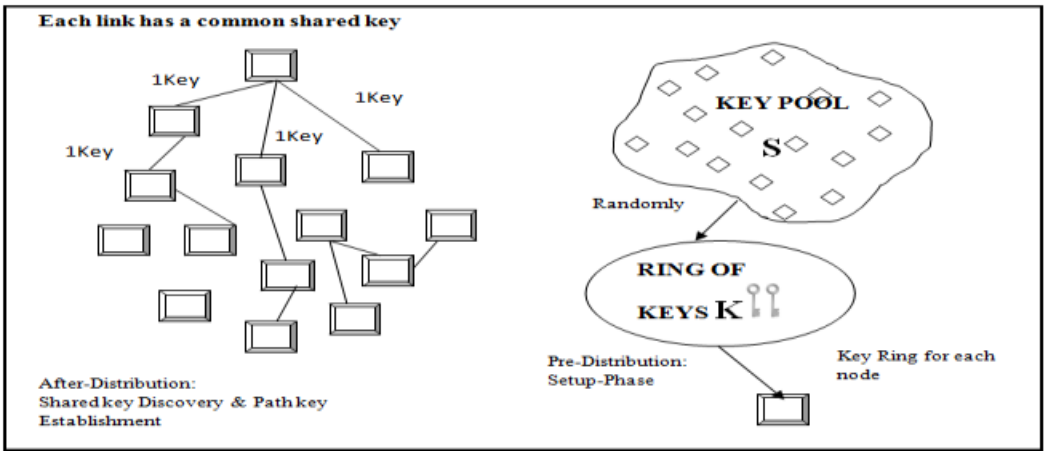

Fig. 1.2: Pair Wise Key Establishment.

C. Trusted Key Distribution Center:

In this scheme, a trusted third party is used which can either be a sensor node within the network or a base station. The trusted server contains all pair-wise keys and the key is distributed between the nodes, whereas in the pair-wise key establishment, keys are preloaded on the sensor nodes. It is applied to small networks. It is easy to add and remove entities from the network. Each entity needs to store only one long-term secret key.

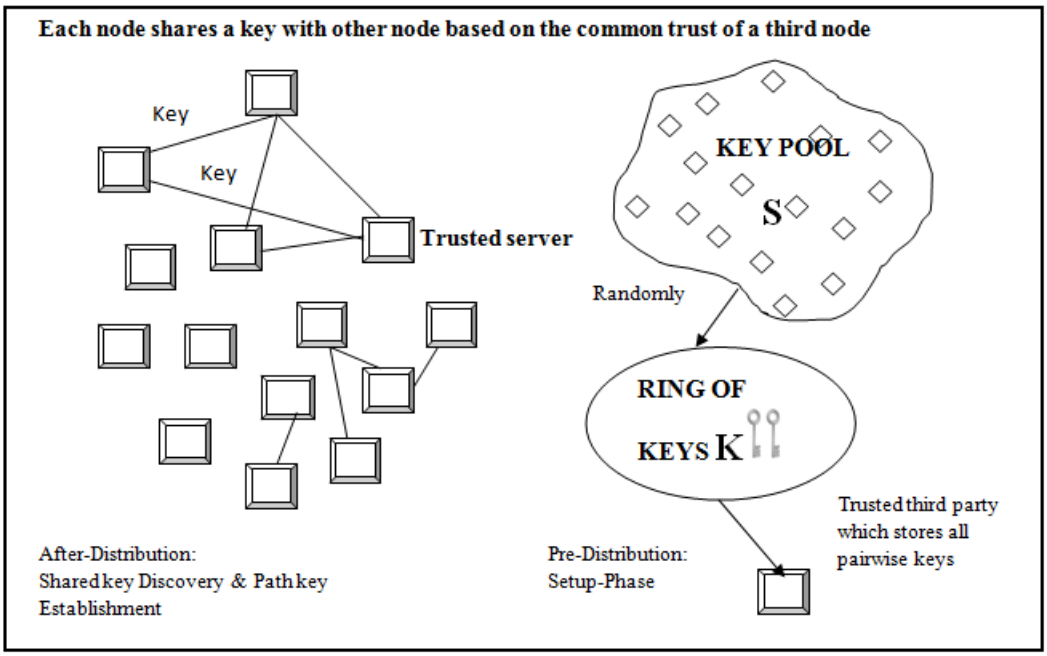

Fig. 1.3: Trusted Key Distribution Center.

D. Q-composite Key Pre-distribution (QKP):

Q-composite approach is the enhancement of the basic probabilistic approach, which achieves strengthened security against small scale attacks. Here, the nodes in the network should share q keys instead of only one. In this approach, key pool is an ordered set. During the initialization phase nodes broadcast identifiers IDs of keys that they have. After the discovery of each node identifies the neighbor nodes with which it shares at least q number of keys. Hence, the key for communicating purpose is computed by hashing all shared keys. The keys appear in hash in the same order as in key pool. Q-composite approach has greater resiliency to node capture than the basic approach if a small number of nodes were captured. However, if a large number of nodes have been compromised q-composite scheme exposes a larger portion of the network. Obtaining the information would be difficult if q value is larger.

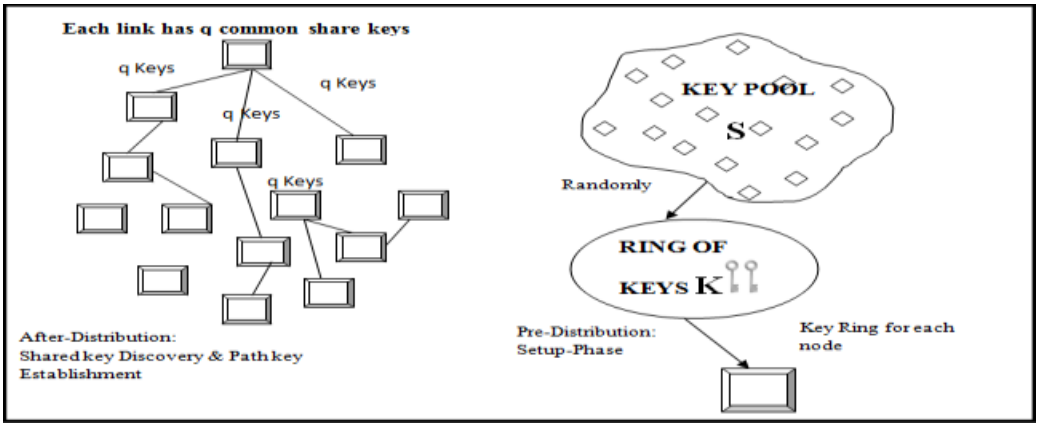

Fig. 1.4: Q-Composite Key Pre-distribution.

E. Transitory master key (TMK):

In this approach, the master key is pre-configured in each sensor node. In order to generate the pair-wise keys, network nodes share the master key with the neighbor nodes. The master key is erased from its memory after a time period [7 ,8]. If the master key is stored in flash memory or even in volatile RAM, the adversary can easily be retrieved. If the master key is computed before it has been erased, then the adversary will obtain all pairwise keys generated. Hence, it is a single point of failure. This causes lots of misbehaving nodes in the network.

F. Opaque transitory master key(OTMK):

The opaque transitory master key is the enhancement of transitory master key. The opaqueness and the inoculation property are preserved even though the master key is compromised [8]. The flexibility of OTMK allows adding of nodes after the master key has been erased. The master key, compromising chances can be reduced by limiting the time period

G. Random pair-wise Key Pre-distribution (RPKP):

This scheme distributes a random number of keys selected from a pool for each sensor node. Nodes communicate with each other only when they have a shared key [6]. During the initialization, every node verifies with its neighbor node by sharing a key with it. When a node is captured, only part of the network is compromised. This approach targets node-to-node authentication without any help from the base station. Each node needs a random set of n*p keys instead of all n-1 keys, where p is the smallest probability that any two nodes have a shared key such that all nodes have shared keys with some high probability. Nodes are pre-deployed with m random pair-wise keys for m other nodes. The node broadcasts its identifier once deployed. Mutual key agreement with the neighbors takes place by cryptographic handshake. Multi-hop range extension is simply by having neighbors rebroadcast the identifiers further and must be used for a limited number of hops to prevent DoS attack by an adversary. Distributed node revocation is possible by having nodes broadcast public votes against a misbehaving node that is a mechanism for detecting misbehavior assumed at each node. If A receives more than a threshold number of votes are against B, it cuts off all communication with B. Node replication can be resisted by limiting the max degree of each node as the Degree counting is modeled in a similar way as vote counting for node revocation. Complete resilience against node capture as the compromised node does not provide any further information. Finally, the large network size supported.

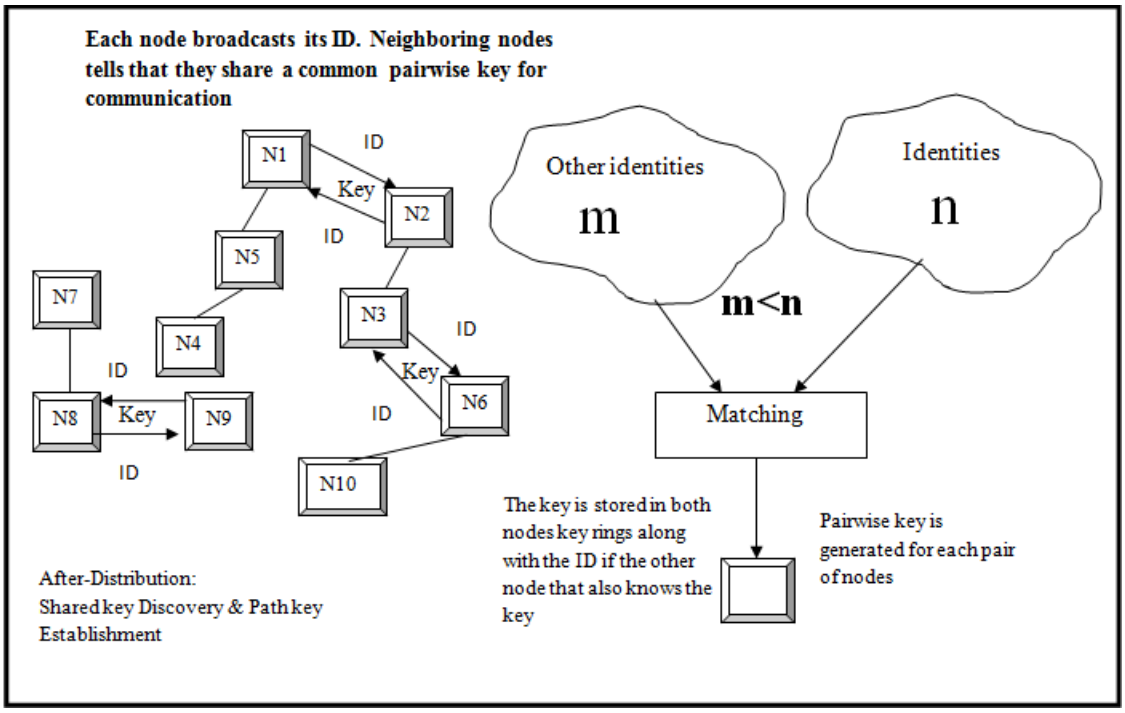

Fig. 1.5: Random Pair-wise Key Pre-Distribution.

H. Multipath key reinforcement scheme(MPKR):

It increases the security as many no of nodes should be compromised to achieve compromising of the communication. Need to update the key once a secure link has been formed between two nodes in order to

prevent an attacker from obtaining and using the old key to capture the other nodes. Node A sends j random values over multiple disjoint secure paths to node B. The new key is computed from all the j values. The attacker has to eavesdrop on j paths in order to construct the key. The neighbors on those paths are called reinforcing neighbors. The method is not as effective when used with q-Composite. Both the methods approximately do the same thing, but their weakness compound each other, such as Small key pool and high network overheads whereas it works well in conjunction with the basic scheme by reducing the eavesdropping probability times.

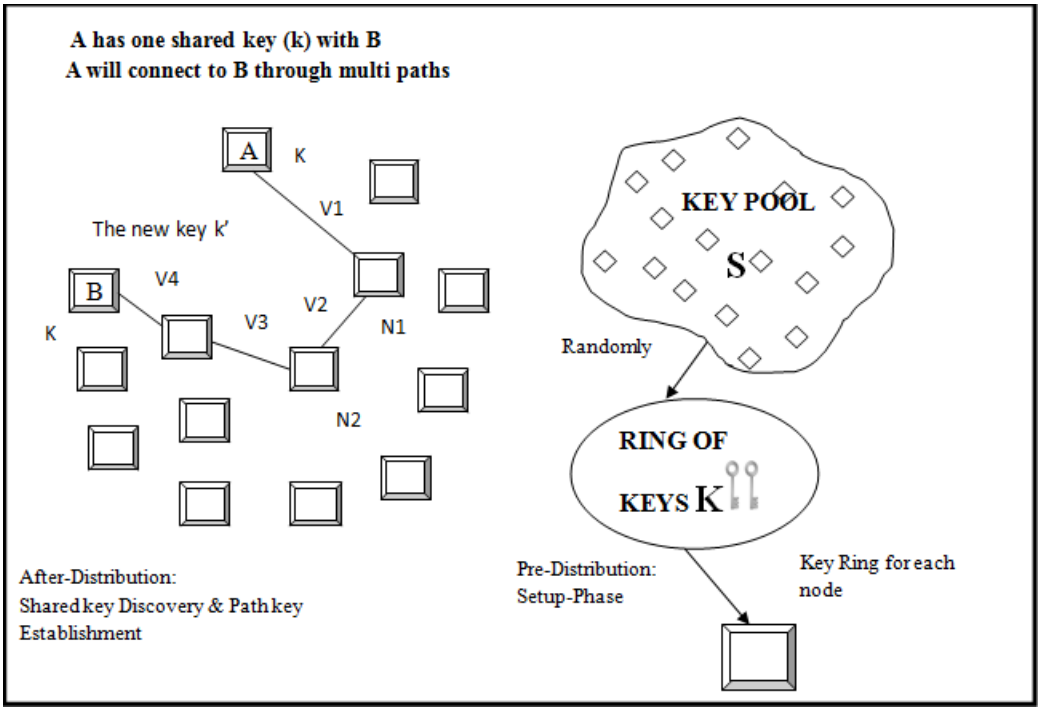

Fig. 1.6: Multipath Key Reinforcement Scheme.

I. Knowledge Based Key Pre distribution (KBKP):

Knowledge based key pre-distribution scheme is the basic scheme that distributes keys prior to the deployment. In the key initialization phase, it provides pieces of information called the node deployment knowledge prior to network deployment. In the key establishment phase, nodes broadcast its identifier ID and establish a shared key based on the prior information [4]. Node deployment knowledge gives the knowledge about the nodes position and its neighborhood information. Nodes shares the keys assigned to it with its neighboring nodes.

J. Polynomial pool based key pre-distribution scheme (PPBKP):

Polynomial pool based key pre-distribution uses a pool of randomly generated bivariate polynomial phases has three phases such as setup phase, direct key establishment phase and path key establishment phase [5]. In the Setup (Pre-distribution), the setup server randomly generates a set *F* of *t*-degree polynomials over the finite field Fq. For each sensor node, the server picks a subset of polynomials and initializes every sensor by distributing polynomial shares to them. Within the Direct Key Establishment, sensors attempt to set up direct keys. If both sensor shares the common polynomial, they can establish the pair-wise key directly. Polynomial share discovery is used to find a common polynomial of which both sensors have polynomial shares using pre-distribution and real-time discovery. The Path Key Establishment is the third phase that establishes pair-wise keys with the help of other adjacent nodes in the path. It has no communication overhead and is unconditionally secure for up to t compromised nodes, but can't only tolerate not more than t compromised nodes. Polynomial pool based key pre-distribution scheme is classified as: Random subset assignment scheme is the scheme that provides a higher probability for sensors to establish secure communication. Unless the number of compromised nodes is greater than the threshold, capturing of sensors does not lead to the disclosure of other keys. In Grid-based key pre-distribution scheme, two nodes can establish a pair-wise key when there is no compromised node. No communication overhead during the discovery of shared keys.

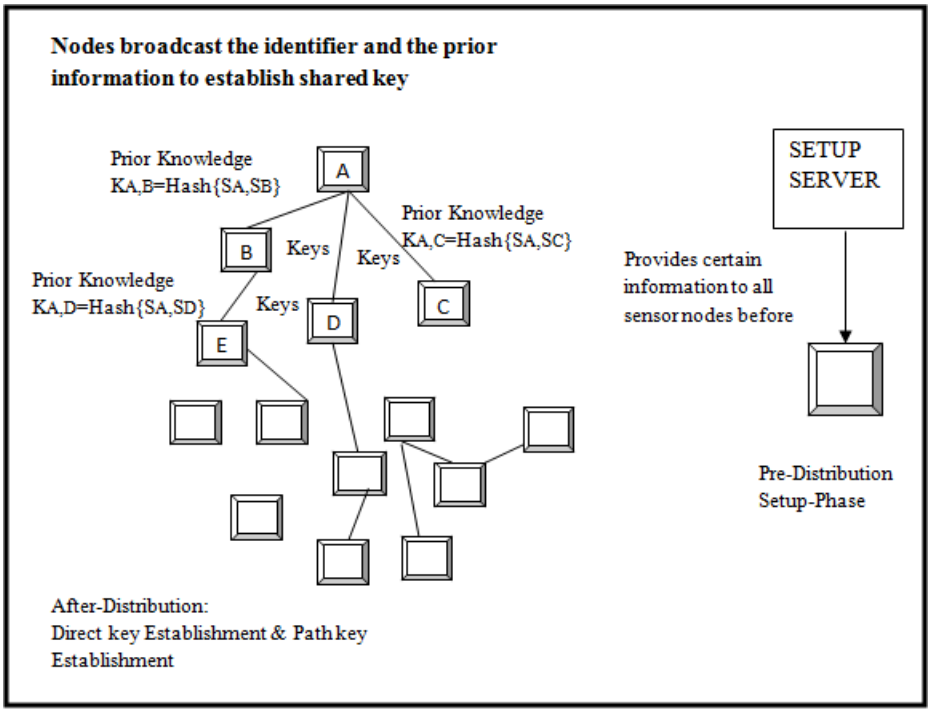

Fig. 1.7: Knowledge Based Key Pre Distribution.

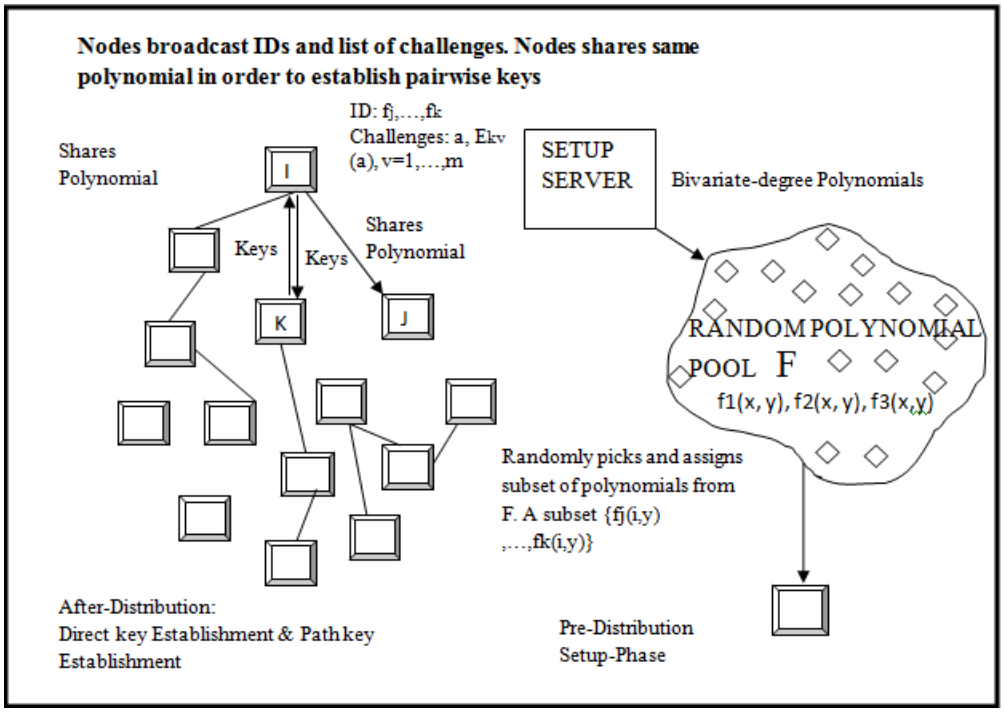

Fig. 1.8: Polynomial Pool Based Key Pre-Distribution Scheme.

IV. Proposed Scheme:

Random seed distribution with transitory master key employs the establishment of a large probability of keys using a small pool. RSDTMK approves all types of keys provided by LEAP+. Before network deployment, data's are distributed to each node and the configuration is done. Each node is provided with the details such as the ring of seeds, the key transformation function, the master key MK, the node identifier IDi, the length permutation factor and the time period of initialization phase. The initialization phase starts at the activation of the node and lasts for a limited period. During the initialization phase, every node broadcast a hello message with its IDA (node, id) and IDSx (seed identifier).When the neighbor node receives a hello message, it looks for

shared seeds. If the shared key is found, then permutation factor is selected Node generates a new key for each seed still not used, which in turn generates at least a key for each seed. The shared seed is used to generate a pair-wise key between the nodes with the permutation function and key transformation function. At the end of the initialization phase, the node erases the whole secret material which is only required in this phase to protect the security of the network. Nodes cannot even generate keys after initialization phase. Hence, for secure connection, it uses the keys that are generated at the initialization phases. Establishing key between nodes in initialization phase and another node in working phase is used for the addition of new nodes in the network. In the working phase, the nodes contain a ring composed of keys rather than ring composed of seeds. Finally, pair-wise keys are generated for network communication

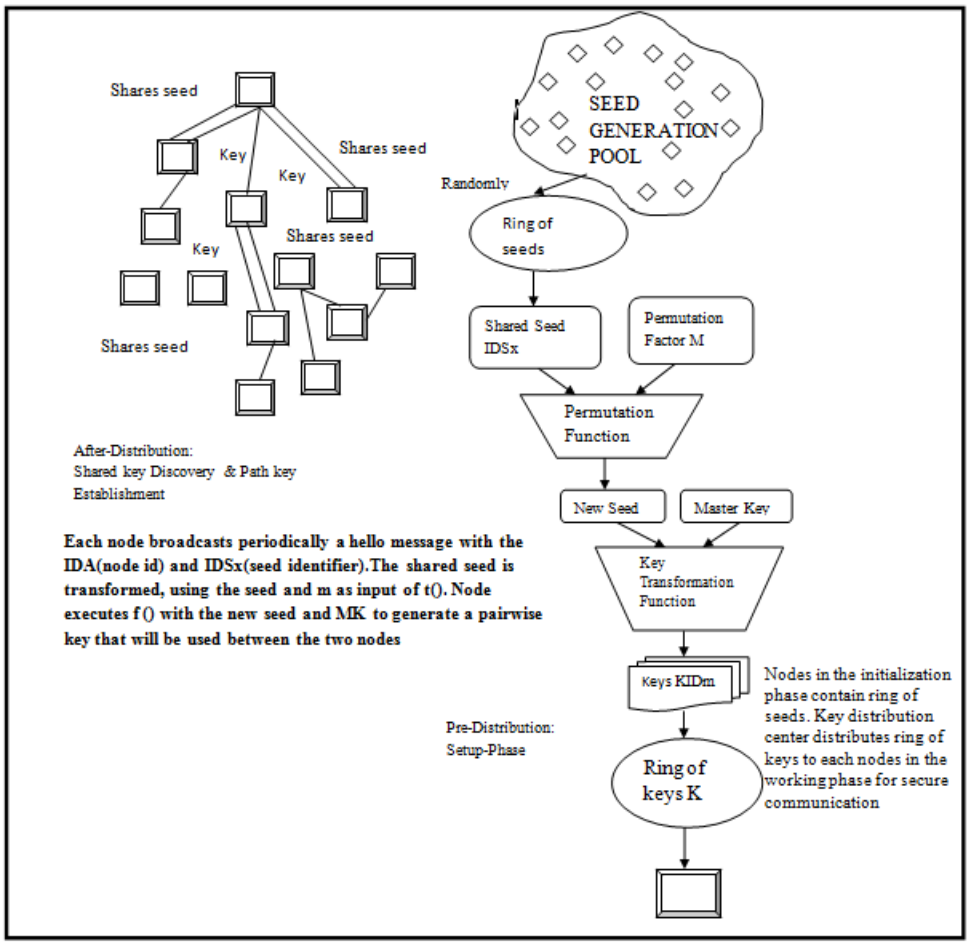

Fig. 1.9: Random Seed Distribution with Transitory Master Key.

V. Comparison:

Key management scheme analyzes the performance based on the evaluation metrics [2].

A. Resilience:

Resilience is an action that provides toughness and the effects due to the compromised secret material are lower. Resilience is the major metric that ensures the security level of each scheme. Q-composite key pre-distribution scheme (QKP) [6], Transitory master key (TMK) [7] and pair-wise key establishment (PKE) provides best resilience against one compromised key. Random seed distribution with transitory master key (RSDTMK) provides high resilience without limiting the connectivity, but random pair-wise key pre-distribution (RPKP) provides good resilience when the pool of keys is larger, but it affects the connectivity. The RPKP is less robust than QKP when several nodes are compromised whereas other schemes resilience remains the same.

B. Connectivity:

Connectivity refers to the establishment of communication between nodes by sharing the secret material. TMK, PKE and SNWK provide better connectivity; whereas the connectivity of RPKP and QKP is based on the probability of adversaries compromise the nodes. RDSTMK provides connectivity same as TMK.

C. Mutual Authentication:

Mutual Authentication occurs between the nodes in the network so that the unauthorized entities are prevented from gaining the access. TKP, MPKR, TMK and RSDTMK ensures mutual authentication, whereas other schemes doesn't ensure authentication.

D. Memory:

Memory space required to store keys, information, identifier ID and some parameter should be limited. SNWK, PKE, MPKR and TMK deals with the memory constraints SNWK is shared by all the authorized nodes and if any, authorized node is compromised adversaries can eavesdrop. In TKP, all communication requires initial interaction with the trusted third party (TTP). The TTP must be trusted to store n long-terms keys and should have the ability to read and forge all messages if the TTP is compromised, all communications are insecure. TMK satisfies the requirements only if the master key has not compromised and if it is compromised, then it is the single point of failure of the whole system. OTMK preserves opaqueness of the master key and drawback of OTMK is that a node cannot immediately make sure of whether the pair-wise key has really set up. RPKP lacks authentication process and nodes are unreachable since every node is not guaranteed to have common key to its neighbors. Q-composite random key pre-distribution scheme, nodes share not just one common key, but q common keys to preserve node capture yet capturing a few nodes, the network is jeopardized. In MRK, secure links formed using a common key, and then if any node compromised then whole network is threatened. PPBKP allows the network to grow to a large size after deployment, but compromising more than t polynomials leads to the network compromise. LEAP offers efficient protocols for supporting types of key schemes of different types of messages broadcasted, reduces battery usage and communication overhead, but requires excessive storage with each node storing four types of keys. Nodes in the network can communicate with its neighbor nodes, when the size of the key ring is too large, but it causes adversaries to capture part of network by compromising node and also memory usage. Nodes would not be able to communicate with any neighbor, when the size of the key ring is too small. In the RSDTMK, the number of possible keys in the network is higher than in the ring with respect to the pool. The effects due to the compromised secret material are lower. RSDTMK provides connectivity without limiting the resilience and increase in the quantity of possible key in the network.

Table 1: Comparison of Key Management Schemes.

ABBREVIATION OF THE SCHEMES	PERFORMANCE CHARACTERISTICS						
	RESILIENCY	*OVERHEAD*	*SCALABILITY*	*MOBILITY*	*MEMORY*	*MUTUAL AUTHENTICATION*	*CONNECTIVITY*
SNWK	Reduced resiliency	Less overhead, since single key is used	Reduced scalability	Handles node mobility	Deals with memory constraints	Doesn't ensure mutual authentication	Best connectivity
PKE	Resiliency has been improved	Less overhead	Provides scalability	Handles node mobility	Memory constraints are handled	No mutual authentication	Best connectivity
TKP	Reduced resiliency	More overhead	Reduced scalability	Can't handle node mobility	Can handle memory constraints	Ensures mutual authentication	Less connectivity
RPKP	Resiliency is reduced	Less overhead	Infinite scalability	Ensures node mobility	Can't deal with memory constraints	Can't ensure mutual authentication	Less connectivity
QKP	Improved resiliency	More overhead	Offers scalability	Offers node mobility	Can't deal with memory constraints	Can't ensure mutual authentication	Less connectivity
KBKP	Less resiliency	Less overhead	Scalability is reduced	Can't ensure node mobility	Can't deal with memory constraints	Can't ensure mutual authentication	Less connectivity
MPKR	Improved resiliency	More overhead	Offers scalability	Offers node mobility	Can deal with memory constraints	Can ensure mutual authentication when it is in conjunction with random pairwise key pre-distribution	High connectivity
PPBKP	Increased resiliency	More overhead	Offers infinite scalability	Ensure node mobility	Can't deal with memory constraints	Can ensure mutual authentication	High connectivity
TMK	Increased resiliency	More overhead	Offers scalability	Can't ensure node mobility	Deals with memory constraints	Ensure mutual authentication	Best connectivity
OTMK	Increased resiliency	Less overhead	Offers Infinite scalability	Can't ensure node mobility	Deals with memory constraints	Ensure mutual authentication	Best connectivity
RSDTMK	High level of resiliency	More overhead	Offers infinite scalability	Can ensure node mobility	Can't deal with strict memory constraints	Ensure mutual authentication	Best connectivity

VI. Conclusion:

Key management schemes play an important issue that has been used in various networks for security purpose and many other new schemes were found. Different key management schemes must be found out which provides high resilience, robustness to the network with limited resources and overhead. All the schemes have some advantages as well as some disadvantages. Future research should aim for the avoidance of compromised nodes.

REFERENCES

[1] Xiangqian Chen, Kia Makki, Kang Yen, And Niki Pissinoum, 2009. "Sensor Network Security: Survey", IEEE Communications Surveys & Tutorials, vol. 11, no. 2, Second Quarter.
[2] Lee, J. *et al*., 2007. "Key management issues in wireless sensor networks: Current proposals and future developments," IEEEWireless Commun., 14(5): 76-84.
[3] Stallings, W., 2003. "Cryptography and Network Security- Principles and Practices", 3rd ed. Upper Saddle River, NJ: Prentice Hall.
[4] Deng, Y.S. Han, S. Chen and P.K. Varshney, 2004. "A Key Management Scheme for Wireless Networks Using Deployment Knowledge", In The 23rd Conference of the IEEE Communications Society (Infocom),Hong Kong.
[5] Chan, H., A. Perrig and D. Song, 2004. "Key Distribution Techniques for Sensor Networks", Wireless Sensor Networks, pp. 277-303, Kluwer Academic.
[6] Chan, H., A. Perrig and D. Song, 2003. "Random key predistribution schemes for sensor networks," in Proc. Symp. Security and Privacy, pp: 197-213.
[7] Zhu, S., *et al*., 2006. "Leap+: Efficient security mechanisms for large-scale distributed sensor networks," ACM Trans. Sensor Netw., 2(4): 500-528.
[8] Deng, J., C. Hartung, R. Han and S. Mishra, 2005. "A practical study of transitory master key establishment for wireless sensor networks," in Proc. 1st Int. Conf. Security and Privacy for Emerging Areas in Commun. Netw., Washington, DC, USA, pp: 289-302.