Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 2, February -2017

EFFICIENT KEY MANGEMENT SCHEME IN WIRELESS SENSOR NETWORKS: AN OVERVIEW

Sri Meenakshi.N[1], Vinitha.R[2], Yuganthi.S[3], Geetha.R[4]

[1,2,3] *UG Student,*[4]*Associate Professor, Department of Computer Science and Engineering, , S.A Engineering College.*

Abstract—*Wireless sensor networks have been widely used in various applications which are widely used by the research area due to their self-configured and infrastructure-less wireless networks but are subjected to various security attacks. It is important to impose some security measures to overcome these issues. Many key establishment techniques have been designed to address the tradeoff between limited memory and security, but which scheme is the most effective is still debatable. A number of key generation and distribution techniques have been discussed in this literature. The various metrics like efficiency, resilience, connectivity, overhead, etc., are compared and analyzed.*

Keywords*—Key management, Wireless Sensor Networks(WSN), Random key pre-distribution, Security, Scalability.*

I. INTRODUCTION

WIRELESS sensor networks (WSN) [12] are used to monitor environmental and physical changes by means of sensor nodes. They are becoming a popular ubiquitous computing. They are used in different applications such as health care monitoring, environmental/earth sensing, air pollution monitoring, forest fire detection, industrial monitoring and many more. Since there are only limited resources, WSNs are exposed to many vulnerable attacks such as false message injection, eavesdropping etc., hence more security measures are needed.

In recent times many techniques such as random key pre-distribution and random pairwise key distribution has been used. The security in WSN has been enhanced by using a symmetric key encryption technique.

Some of the issues related to Wireless Sensor Networks are discussed below. The pros and cons of the issues in WSN has been put forth discussed, compared and evaluated in this survey.

A. Integrity

It is an essential factor to be considered in wireless sensor networks. The data sent by the sender should be received by the receiver without any changes in the data.

B. Confidentiality

Data transferred are subjected to many security attacks such as eavesdropping in a wireless sensor networks. In order to overcome this issue, the cryptographic techniques have been used.

C. Availability

The resources are to be readily available even in case of the Denial of service (Dos) in wireless sensor network. This increases the quality of service (Qos) in the network.

D. Authentication

The data must be authenticated in order to be secure. This is done by using cryptographic techniques by sharing keys.

The Scenario of the Key distribution in Wireless sensor networks(WSN) has been shown in the figure 1. They are represented as different forms like clusters as a dotted circle, Pairs of nodes in different colors, nodes as a circle and ,an arrow as a range between the nodes.

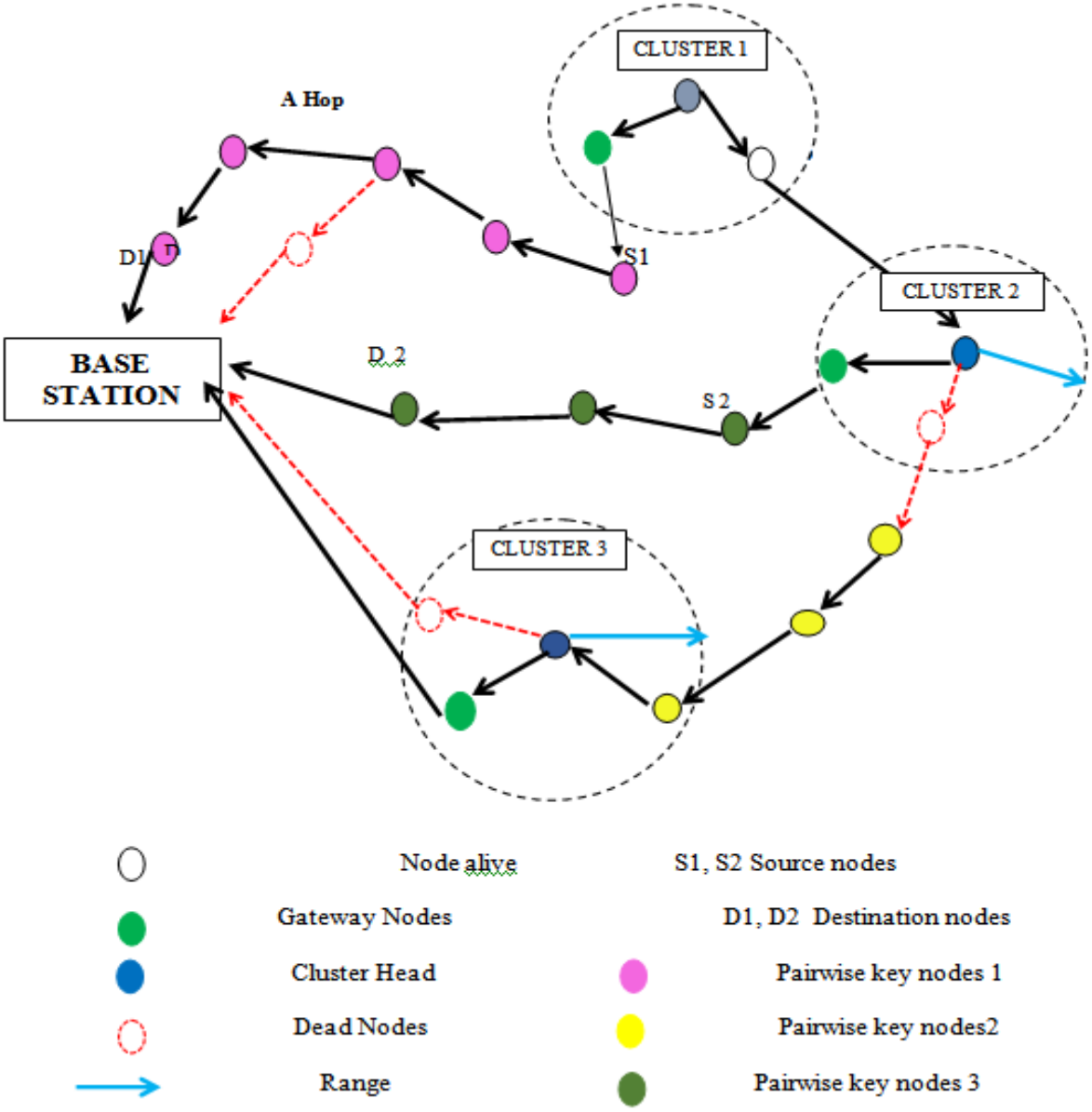

Figure 1.A Scenario of Key distribution in WSN

The data transfer is specified in the above diagram between the source node (s1, s2) and the destination node (d1, d2) from a cluster to base station. Each cluster consists of a cluster head. The pairwise key generation is done between each pair. Two different clusters are connected using gateway nodes. Dead node is a generated node that is not to be expanded or explored.

II.SECURE MECHANISMS USED IN WIRELESS SENSOR NETWORKS

In this section, the various security mechanisms have been proposed. The cryptographic mechanisms are used to overcome the attacks in WSN.

A. Cryptographic mechanism:

The cryptographic mechanism uses a key establishment technique in which the key is shared between the sender and the receiver. This technique must be proposed in such a way that the energy constraints, computational time and scalability must be high.

a. Public key cryptography in WSN: Public key cryptography [4] techniques such as Diffie-Hellman key exchange and RSA algorithm executes in such a way that it executes thousands or millions of instructions to operate a single security operation. Hence the symmetric key cryptography has been put forth which is described below.

b. Symmetric key cryptography in WSN: Symmetric key cryptography [8] is used in network security to overcome the computational overhead. Symmetric key Encryption is the one in which a same key is used for both encryption and decryption by both the sender and receiver. Key distribution is the establishment of the symmetric keys. The main challenge in symmetric key encryption is that how the sharing of keys is done securely. Though the symmetric key encryption is good by low cost and high speed computation, it is less secure in terms of key distribution. So a more promising scheme should be established.

III. RELATED WORK

Wireless sensor networks are dense wireless network of sensor nodes collecting and disseminating environmental data. Sensor nodes are small low-power devices used majorly.
In computation, communication and storage capabilities, mainly for economic reasons. It even has various kinds of promising applications that include environmental monitoring.
In this section, we discuss about location based deployment model, location based pairwise key pre-distribution.

Taekyoung et al. [1], proposes the model that uniquely conceive group hierarchies and subareas that accommodate deployment errors on the group-based deployment model. The overall sensing field is been divided geographically into a regular square zones while different polygons can also be considered via distinct deployment strategies. After deployment based on the possible errors , the zone groups are divided into three subarea groups namely inner, outer and border areas then the node can configure their own one hop subgroup.

Location based pairwise key pre-distribution devises the scheme in three phases with practical concern. These schemes are called as a full and random pairwise key pre-distribution (FRP) scheme that buses deployment knowledge and path key offering method. Here first phase deals with key pre-distribution with deployment knowledge, the second phase deals with shared key discovery and the third phase deals with Path Key Establishment with Path Key Offering.

Gregory et al.[2], proposed a cyber-physical architecture that maps flexibility based damage identification efficiently in a distributed wireless sensor network. Also described the implementation of the same architecture on top of a Tiny OS operating system and ISHM service tool suite. The evaluation of implementation on a stimulated truss structure and a real, full scale truss structure localizes damage on both structures successfully to the resolution of the single element. Efficiency of the approach is experimented through latency and power consumption data collected. It states that the existing research separate's the wireless sensor networks and structural engineering algorithm , thus a cyber-physical co-design approach is proposed to do health monitoring based on wireless sensor networks. The approach integrates flexibility based damage localization, energy efficient multilevel computing architecture. This approach is implemented on Intel Imote2 platform. In a network hierarchy a node selected is assigned with three roles namely cluster member, cluster head, base station. A role of a node is determined by the type of data it handles and its level in the network hierarchy. The system operates based on the roles. The nodes combine to form clusters where each cluster acts as an independent unit, with the cluster head coordinating the nodes within the cluster.

In this section Chia-Mu Yu et al.[3], deals with the node replication problem detection which is challenging these days. Node replication attacks demand immediate attention, when compared to the extensive exploration on the defense against node replication attack, this shows there is only a limited solutions in mobile networks. It states that most of the existing schemes in static networks rely on the witness-finding strategy, which is not possible to be applied in mobile networks, the velocity-exceeding strategy used in existing schemes in mobile networks has efficiency and even security related issues. Therefore, localized algorithms have been proposed in order to resist node replication attacks in mobile sensor networks. The proposed algorithm has advantages such as efficiency and effectiveness, localized detection, network-wide synchronization avoidance and network-wide revocation avoidance. Performance comparisons are provided to demonstrate the efficiency of the proposed algorithms with known methods. Prototype implementation on TelosB mote demonstrates the practicality of the proposed methods.

Seung-Hyun Seo et al.[4], describes that Dynamic wireless sensor networks enables mobility of sensor nodes this facilitate wider coverage of networks and accurate services than static wireless sensor networks. This is rapidly adopted to monitor the applications like target tracking in battlefield surveillance , health care system , vehicle status monitoring, dairy cattle health monitoring. It states that sensor devices are vulnerable to malicious security attacks such as capture, impersonation, interception or physical destruction. This physical destruction is due to their unattended operative environments and lapses of connectivity in wireless communication. This shows security is one of the most important issues in many critical dynamic wireless sensor network applications. Security requirements such as node authentication, data confidentiality and integrity are addressed by dynamic wireless sensor networks whenever and wherever the nodes move. This paper proposes a certificate less-effective key management (CL-EKM) protocol for secure communication which is characterized by node mobility. The proposed protocol supports key updates in an efficient way whenever the node joins or leaves the cluster and also it ensures the forward and backward key secrecy. Finally a security analysis is done which shows that the protocol is effective in dealing with several attacks. CL-EKM is implemented in ContikiOS and it is simulated using Cooja simulator which is used to assess its time, energy, communication and memory performance.

Wenliang Du et al.[5],states that there exist a number of proposed schemes to provide varieties of solutions to key pre-distribution problems; also states that it does not exploit an important piece of information that significantly improves the performance. The node deployment knowledge is derived from the way how the nodes are deployed. The author attempts the use of deployment knowledge in key pre-distribution. This is done by modeling node deployment knowledge in wireless sensor network and then developing a key pre-distribution scheme based on the model. It is shown that key pre-distribution with deployment knowledge can substantially improve a network's connectivity and reduce the amount of memory required. In order to achieve security the messages sent among sensor nodes must be encrypted, this encryption should be agreed upon communicating nodes. Key agreement schemes such as Diffie-Hellman; public key based schemes are not suitable for wireless sensor network. Even the pre-distribution of secret keys consume large memory when it is to be applied to a network which is large in size. Thus the author proposes random key pre-distribution scheme and also its significant are discussed. A common assumption made in this case is no deployment knowledge is available. It also deals with the detailed performance evaluation.

M. Eltoweissy et al. [6], describes the model that dynamically establish and maintain a secure channels among communicating nodes is the main objective of key management. The desired features of key management in sensor networks include localized impact of attacks, energy awareness and scaling to a large number of nodes. A primary challenge in this is managing the trade-off between the acceptable levels of security and conserving scarce resources, in particular energy, needed for the network operations. Schemes such as a static schemes, adopted the principle of key pre-distribution with the underlying assumption that a relatively static short-lived network. An emerging class of schemes and dynamic key management schemes assumes a long-lived network with more frequent addition of less number of nodes, thus the requiring network for sustained security issues and survivability. In this article author presents a classification of key management schemes in sensor networks describing their similarities and differences. It also describe a detailed dynamic key management scheme, localized combinatorial keying (LOCK), and it also compare its security and performance with a representing a static key management scheme. It gives way for future research directions.

In this section Z. Yu Y. Guanet al. [7], proposed several key management schemes in order to implement new security and privacy challenges in wireless sensor networks.one important challenge among this is bootstrapping secure communication among the nodes. It is difficult to offer either a strong resilience against the node capture attacks or it requires excess memory in order to achieve the desired connectivity. Thus the author proposes an efficient key management scheme using the deployment knowledge. In this scheme a field which is targeted is divided into hexagon grids and the sensor nodes are divided into equal number of groups as that of a grids and these groups are deployed into a unique grid. Using the deployment knowledge, a large number of potential groups are reduced from which a node's neighbor can be added. Thus the generation of pairwise key becomes efficient for communication between two nodes. In comparison with the existing scheme this provides higher connectivity with less memory requirement and even a short transmission range. Finally it gives the performance of other schemes in terms of resilience against node capture attacks.
D. H. Yum et al.[8], states that Key management schemes are required for sensor nodes as the wireless sensor networks are mostly deployed in the adverse hostile environments. A probabilistic key management scheme called random key

pre-distribution (RKP) where each node is preloaded with a subset of keys that are randomly selected from a large set of keys. A secure link must be established between two nodes that are neighboring which have a common key. The neighboring nodes must have at least q common keys in order to establish q-composite RKP scheme. The authors state that the security analysis on resilience against node capture of q-composite is inaccurate and also suggests a new scheme to formulate for q-composite RKP scheme and resilience in the RKP scheme.

Since wireless sensor networks are used in several beneficial applications, they subjected to various security threats. The security threats that are possible are eavesdropping and hardware tampering. To achieve secure communication among nodes many approaches are used which involve symmetric encryption. Key management schemes are proposed in order to establish secret keys.

F.Gandino et al.[9], proposes a unique key management scheme called random seed distribution with transistor master key; this master key is used in random distribution of secret material and also to generate pairwise keys. Thus this approach overcomes the drawbacks of the previous approaches based on the technique proposed. It even outperforms the state-of-art protocol in order to provide a high security level. These approaches are mainly used in wireless sensor networks, to manage the keys. The key pre-distribution to the nodes is made without any additional mechanism or deployment knowledge. The key management schemes proposed here are plain global key (PGK) and full pairwise keys (FPWK).

W.Bechkit et al.[10], states that Key management emerges a challenging issue in wireless sensor networks due to the sensitivity of the potential wireless sensor network and the resource limitations. The main issue to be considered is scalability, when designing a key management scheme. So the large scale deployment of the network should support the large number of nodes. The author proposes a new scalable key management scheme in wireless sensor networks to implement a efficient and secure connectivity coverage. Thus a unital design theory is proposed. The unitals are mapped with the key pre-distribution to achieve high scalability. Thus the author proposes an advanced unital based key pre-distribution scheme to provide high network scalability and an efficient key sharing probability. Finally approximate analysis and simulations are performed in order to compare the solutions of existing methods which is based on the criteria such as storage overload, securing average path length, network scalability, network resiliency and network connectivity.

IV. SUMMARY OF THE SURVEY

The above surveys are summarized in the following tables with respect to various metrics and algorithms. Table 1 describes the various protocol related to resilience and connectivity. In this survey most of the protocol provides high connectivity but low resilience which are to be viewed.

TABLE 1.COMPARISON OF RESILIENCE AND CONNECTIVITY

PROTOCOLS	RESILIENCE	CONNECTIVITY
FRP [1]	✓	✓
NOVEL CYBER PHYSICAL CO-DESIGN [2]	×	×
XED AND EDD [3]	×	✓
CL-EKM [4]	×	✓
LOCK [5]	✓	✓
NOVEL KEY MANAGEMENT SCHEME [6]	✓	✓
Q-COMPOSITE [7]	×	✓
UNITAL DESIGN [8]	✓	✓

Table 2 describes about the algorithm type which is either localized or centralized, support network type which is static or dynamic, type of key which is pairwise or cluster key and to know whether a protocol is deployment model or not. These attributes describe the efficiency of that particular protocol.

TABLE 2.COMPARISON OF NETWORK TYPE,KEY AND MODEL

PROTOCOLS	ALGORITHM TYPE	SUPPORT NETWORK TYPE	TYPE OF KEY	DEPLOYMENT MODEL
FRP [1]	LOCALIZED	STATIC	PAIRWISE KEY	YES
NOVEL CYBER PHYSICAL CO-DESIGN [2]	LOCALIZED	STATIC	CLUSTER KEY	YES
XED AND EDD [3]	LOCALIZED	DYNAMIC	PAIRWISE KEY	NO
CL-EKM [4]	LOCALIZED	DYNAMIC	PAIRWISE KEY	NO
LOCK [5]	LOCALIZED	DYNAMIC	PAIRWISE KEY	YES
NOVEL KEY MANAGEMENT SCHEME [6]	CENTRALIZED	DYNAMIC	CLUSTER KEY	NO
Q-COMPOSITE [7]	LOCALIZED	DYNAMIC	PAIRWISE KEY	YES
UNITAL DESIGN [8]	LOCALIZED	STATIC	PAIRWISE KEY	NO

Table 3 describes the efficiency, computational overhead and storage of the protocol. The efficiency deals with communication and energy efficiency of the protocol.

TABLE 3.COMPARISON OF EFFICIENCY,OVERHEAD,STORAGE

PROTOCOLS	EFFECIENCY	COMPUTATIONAL OVERHEAD	STORAGE
FRP [1]	COMMUNICATION EFFICIENT	LOW	HIGH
NOVEL CYBER PHYSICAL CO-DESIGN [2]	ENERGY EFFICIENT	HIGH	LOW
XED AND EDD [3]	ENERGY EFFICIENT	HIGH	HIGH
LOCK [5]	-	HIGH	HIGH
NOVEL KEY MANAGEMENT SCHEME [6]	ENERGY EFFICIENT	HIGH	
Q-COMPOSITE [7]	COMMUNICATION EFFECIENT	HIGH	LOW
UNITAL DESIGN [8]	COMMUNICTION EFFICIENT	LOW	LOW

V. CONCLUSION

Though most of the techniques have been proposed to overcome the security threats through different key management schemes, the issues still exist in the system. The survey focused on variousWSN characteristics such as energy constraints, communication capability, bandwidth and memory. The summary also discussed the metrics such as resilience and connectivity of the various schemes. The design of the key management techniques should satisfy all these constraints. Hence a technique that holds all the characteristics should be introduced. Most of the techniques deal with the individual security issues but they do not satisfy all the requirements.

VI.REFERENCES

[1]T.Kwon J. Lee J. Song "Location-based pairwise key pre-distribution for wireless sensor networks" IEEE Trans. Wireless Communication. vol. 8 no. 11 pp. 5436-5442 Nov. 2009.

[2]G.HackmannW.Guo G. Yan Z. Sun C. Lu S. Dyke "Cyber-physical co-design of distributed structural health monitoring with wireless sensor networks" IEEE Trans. Parallel Distribution Syst. vol. 25 no. 1 pp. 63-72 Jan. 2014.

[3] C.-M. Yu Y.-T. Tsou C.-S. Lu S.-Y.Kuo "Localized algorithms for detection of node replication attacks in mobile sensor networks" IEEE Trans. Inf. Forensics Security vol. 8 no. 5 pp. 754-768 May 2013.

[4] S. H. Seo J. Won S. Sultana E. Bertino "Effective key management in dynamic wireless sensor networks" IEEE Trans. Inf. Forensics Security vol. 10 no. 2 pp. 371-383 Feb. 2015.

[5]Wenliang Du, Jing Deng, Yunghsiang S. Hans, and Pramod K. Varshney, "A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge" IEEE transactions on dependable and secure computing, vol. 3, no. 1, january-march 2006.

[6] M. Eltoweissy, M. Moharrum, R. Mukkamala, "Dynamic key management in sensor networks", *IEEE* Communication. *Mag.*, vol. 44, no. 4, pp. 122-130, Apr. 2006.

[7] Z. Yu Y. Guan "A key management scheme using deployment knowledge for wireless sensor networks" IEEE Trans. Parallel Distribribution. Syst. vol. 19 no. 10 pp. 1411-1425 Oct. 2008.

[8] D. H. Yum P. J. Lee "Exact formulae for resilience in random key pre-distribution schemes" IEEE Trans. Wireless Communication. vol. 11 no. 5 pp. 1638-1642 May 2012.

[9]F.Gandino B. Montrucchio M. Rebaudengo "Key management for static wireless sensor networks with node adding" IEEE Trans. Ind. Information. vol. 10 no. 2 pp. 1133-1143 May 2014.

[10]W.BechkitY.ChallalA.BouabdallahV.Tarokh "A highly scalable key pre-distribution scheme for wireless sensor networks" IEEE Trans. Wireless Communication. vol. 12 no. 2 pp. 948-959 Feb. 2013.

[11]A.K. Das, "Improving identity-based random key establishment scheme for large-scale hierarchical wireless sensor networks", *Int. J. Netw.Secur*, vol. 14, no. 1, pp. 1-21, 2012.

[12]FilippoGandino, Renato Ferrero, Maurizio Rebaudengo, "A Key Distribution Scheme for Mobile Wireless Sensor Networks: q-s composite", IEEE Transactions on information forensics and security, vol. 12, No. 1,January 2017.

