



A Review of Efficient Dynamic Key Management Scheme for Heterogeneous Wireless Sensor Networks

ITFAQ AHMAD MIR^{1*}, G. M. MIR² and MUDASIR AHMAD MAKHDOOMI³

¹ARIS, SKUAST-Kashmir, Srinagar, J&K, 190025, India.

²College of Agri. Engineering., SKUAST-Kashmir, , Srinagar, J&K, 190025, India.

³Department of Computer Sc., ICSC, University of Kashmir, Srinagar, J&K,190006, India.

Abstract

Security has been one of the most critical concerns for wireless sensor network (WSN) systems in recent years. Application of WSN has faced criticism in several fields due to limited flexibility and security in the long term. This study aimed at reviewing the dynamic key management schemes for Heterogenous WSN systems to determine efficient management schemes. Applicability of notable schemes such as Basic scheme, and hybrid schemes under dynamic key management depends majorly on the central key controller presence.



Article History

Received: 22 April 2020

Accepted: 22 May 2020

Keywords

Dynamic Key Management, Distributed Schemes; Heterogenous Wireless Sensor Networks System,

Introduction


Advancements made in communication technologies, computing, and sensing supported with the development of facilities to continuously monitor changes have led to the emergence of Wireless Sensor Networks (WSNs) in the mid-20th century. Reliance on the smart environment for day-to-day needs promoted the deployment of these networks for not only supporting the data acquiring process from different locations but also to have an effective distribution of information's for facilitating other applications to deal with real-time issues like battlefield surveillance, environmental monitoring, healthcare system tracking, smart homes or vehicular traffic management.¹⁻³ Consisting of

four components; radio, sensor, processor, and battery, the WSN system nodes have capabilities to formulate appropriate structure in order to perform collaboratively. Revolutionizing communication and information technology, WSN systems help in granularity tracking of things even when they are going on at inaccessible locations and far-away places. Despite these benefits, WSM system has certain associated constraints i.e. cost, limited battery power, limited computational capability, large scale of deployment, memory limitation, communication bandwidth and range limitation, and physical size of nodes.³ Due to these limitations, WSN systems bear security challenges, limiting its applicability in environment monitoring, military

CONTACT Itfaq Ahmad Mir ✉ itfaq2015@gmail.com 📍 ARIS, SKUAST-Kashmir, Srinagar, J&K, 190025, India.



© 2020 The Author(s). Published by Oriental Scientific Publishing Company

This is an  Open Access article licensed under a Creative Commons license: Attribution 4.0 International (CC-BY).

Doi: <http://dx.doi.org/10.13005/ojst13.0203.01>

fields, hazardous areas, and medical treatment. Security is the crucial issue for WSN systems.⁴⁻⁶ Therefore, there is constant extensive research and development taking place towards key management of security.⁷

Most security protocols are based on authentication algorithms and strong encryption. For ensuring security, key management is fundamental function as sensor nodes for cryptography mechanisms need valid common key.⁸ Herein, key management can be defined as "the set of mechanisms and processes supporting key establishment and maintenance of keying relationship between respective parties as per security policy".⁹ Generally key management schemes are divided into two categories; static (cryptographic keys pre-distributed in sensor codes and remain same throughout sensor nodes lifetime), and dynamic (secret keys changing throughout lifetime).¹⁰ Several key management schemes were proposed time-to-time for WSN security such as Eschenauer and Gligor proposed E-S scheme, Chan stated q-composite scheme, and dynamic calculation based schemes i.e. matrix based key pre distribution scheme and polynomial based key pre distribution scheme.⁷ These schemes have faced appreciation as well as criticism over the years.

In case of homogenous WSNs (system with sensor codes of same capabilities), the key management problem is widely addressed. Though sensor network technology deployment has stated three categories of key management i.e. asymmetric, symmetric, and hybrid and many efficient solutions were made available under these categories, balance between resource consumption and security remains a main problem[8]. The property of heterogeneous cluster based WSN of topology hierarchical require the presence of hierarchical key management for the system.¹¹ Heterogeneous WSN system are equipped with high capacity memory batteries and storage, powerful processor, and ability to communicate on larger distance, tend to provide more benefits compared to homogeneous system thus, key management schemes for them could help in better results derivation.⁸

Currently there is presence of researches on static key management schemes, homogeneous WSNs and pre-distribution schemes. However, the problem with these schemes are the mounting amount of

weaknesses against node compromise,¹² lack of memory storage (Boubiche *et al.*, 2020), non-availability of high communication facility,¹⁴ and non-scalability after deployment.¹⁵ Thus, this study aims at examining the dynamic key management for heterogeneous WSN systems.

Related Work and Contribution

WSN systems are widely used communications platform with the availability of key management schemes to regulate security. However, many research studies in this area were focused on generally developing a key management protocol. For instance, Camtepe & Yener (2008) focused on key management solution for hierarchical and distributed sensor networks by discussing about deterministic, probabilistic, and hybrid key management solutions. WSN wherein Alagheband & Aref (2011) proposed a scheme based on signcryption and cryptography method for hierarchical heterogeneous WSN. Kodali *et al.* (2013) defined usage of hybrid key management scheme in order to reduce energy and computational cost but at memory overhead expense. Elquay *et al.* (2017) discussed about symmetric and asymmetric key management schemes by focusing mainly on pre-distribution schemes; and Manikanthan & Padmapriya (2019) stated a multi-level key management protocol for secure communication, key memory storage, and accuracy derivation in results over clustered WSN. Further, with the knowledge of relevance of heterogeneous system over homogeneous one, the focus shifted towards exploring the key management schemes for heterogeneous. Yuan *et al.* (2020) proposed a key management scheme based on PF-IBS (pairing-free identity based digital signature) algorithm to provide a more safer and energy efficient authentication medium.

Despite widespread exploration of key management schemes, there have been limited studies on the dynamic key management for heterogeneous WSN (HWSN) systems. HWSN systems offer better communication and more efficient information, making them superior to regular WSNs. This paper explores the concept of dynamic key management for heterogeneous WSN by reviewing the currently available different heterogeneous WSN models, different metrics used for evaluation, describing about the researches and development made in dynamic key management securities, discussing about key

pre-distribution protocols, and having the mechanism for performance evaluation of the schemes. This information can be helpful in optimizing security mechanism for heterogeneous WSN by identifying efficient dynamic key establishment algorithms.

Discussion

Heterogeneous Wireless Sensor Networks (Wsn) Models

A heterogeneous network is a combination of various network technologies that help derive efficient data across the network. Illustrating the coexistence and integration with different protocol stacks of wireless

access technologies, a heterogeneous network supporting various applications and services provide multi-mode capabilities of accessing networks.²² Heterogeneous wireless sensor network (HWSN) is represented as the network of sensors with different capabilities and a wireless link with the dissimilar range of communication; for instance, a system with communication technology of ZigBee, IEEE802.11, and IEEE802.3. The difference in sensors capabilities herein is due to presence of different nodes with difference in their sensing range or variation in computational capability.²³

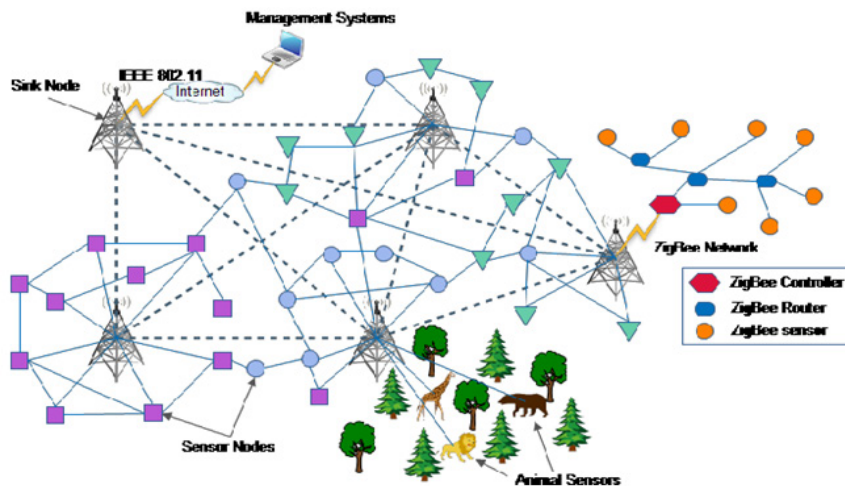


Fig. 1: Heterogeneous WSN model

High-end sensor node under HWSN helps in longer sensing range or communication with the presence of high process throughput. On the other hand, a low end sensor node provides low communication or sensing range, but also has a low process throughput.²⁴ Thus, the HWSN models provide the possibility of using combination of these two nodes tend to support the application by having balance between the cost associated with the WSN usage and the performance of WSN. HWSN have three types of resource heterogeneity (Lee, Krishnamachari, & Kuo, 2004; Yarvis et al., 2005):

Computational Heterogeneity

With the presence of more powerful microprocessor and memory as compared to the normal nodes, the computational heterogeneity defines that HWSN are able to afford longer term storage and complex data processing.²⁵

Energy Heterogeneity

Being the most important heterogeneity for HWSN due to dependence of working on extra energy, the energy heterogeneity defines that HWSN have expandable battery or their line is powered.²⁴

Link Heterogeneity

Long distance network transceiver and high bandwidth in comparison to normal node, the HWSN support data transmission process by adding consistency.²⁴

Due to these, the usage of HWSN has increased in various fields and have contributed by rise in stability, energy efficiency derivation, and raising the network lifetime. Reducing the waiting time (Link Heterogeneity) and processing latency (Computational Heterogeneity), HWSNs decrease retort time.^{24, 27} Further, controlling the energy

consumption, the lifetime of the sensor nodes increase, hence contributing towards prolonging network lifetime, decreasing latency of data transportation, and reliability improvement in data transmission process. Thus, HWSN systems serve as an effective source of network service.²⁴

Evaluation Metrics

The key management systems provide the set of methods which could be used for distributing, creating, and managing the cryptographic keys for WSN security. They provide facilities such as integrity, confidentiality, flexibility, scalability, revocation, resilience, and resistance against nodes;²⁸ the key management system resolves the problem of distribution, maintenance, and generation of secret keys in effective and efficient manner.²⁹ Dynamic key management is a brand of key management for effective security systems and need to possess all these characteristics. Thus, herein, most common metrics used for evaluating dynamic key management of HWSN are as follows.

Security Metrics

Secure encryptions need to be provided by the dynamic key management in order to prevent activities like malicious nodes. In case of detecting a compromised sensor node, there is a need that compromised sensor code key should be revoked along with having generation and distribution of new key related to nodes. Node revocation helps in preventing compromised nodes from influencing network behavior by any manipulation. Following it is the possession of forward and backward secrecy wherein forward secrecy would prevent the node to use old key for new messages decryption while backward secrecy prevents new key from returning to previously received messages and decipher them hence contributing in protecting

against capturing attacks. Further with presence of collusion resistance, technique prevent collaboration of compromised nodes and newly joined while the resilience helps in determining the resistance present against node capturing as network recovery would be easy if intruder could not affect any other node other than captured one (generated key on detection of compromised sensor node).³⁰

Efficiency Metrics

Due to limited nodes storage capacity, network size, and energy resource; there is need that exchanged message for key changing, encryption keys size, operations amount, and required encrypted keys number should be low. This would help in efficient usage of resources by avoiding large loads imposition on bandwidth (size and number of messages exchanges in node eviction, node replenishment, or key generation process), memory (amount of memory needed for having storage of security credentials like trusted certificates, keys, or user certificates), and energy (amount of energy consumed in processes like transmission, data reception, key agreement, or computational procedure of distributing and generating keys).⁹

Flexibility Metrics

These should be flexibility presence in WSN for performing more efficiently. Thus, there should be inclusion of mobility (distribution of new keys to moved nodes for building in better communication), scalability (scalable dynamic key management techniques required for different network sizes along with maintenance of efficiency and security features for small networks), and key connectivity (key connectivity is probability of having two or more nodes deploying key after rekeying. In order to provide continues security, there is requirement of high key connectivity presence).³¹

Highly Storage efficient schemes	Storage efficient schemes	Storage Inefficient schemes
<ul style="list-style-type: none"> • MAKM • SKM • Master key based scheme 	<ul style="list-style-type: none"> • Deployment knowledge based scheme • SHELL 	<ul style="list-style-type: none"> • Basic scheme • q-composite scheme • HC q-composite scheme • Hybrid scheme

Fig. 2: Dynamic Key management schemes

Dynamic Key Management Schemes

Dynamic key management schemes are referred to as key management schemes that change their

administrative keys periodically based on node capture detection or on demand.³² The scheme with their ability to support timely replacement

of captured key, the networks witness enhanced survivability advantage and support for better network expansion.^{33, 34} They are more resilient in node capturing attacks, hence have gained vast popularity in WSN system. These schemes mainly include storage overhead per node, signal range, resilience, location information, and collusion resistance. Extensive research and rising popularity resulted in identification of three types of schemes i.e. storage efficient schemes, storage inefficient schemes, and highly storage efficient schemes.^{35, 36}

However, based on the functionality of the central key controller i.e. its usage for distribution or the new key generation; all dynamic key management schemes for HWSN could be divided broadly into two categories - centralized and distributed schemes.⁹

Distributed Dynamic Key Management Schemes

A distributed dynamic key management scheme refers to a set of processes wherein no central key controller like third party or based station is required for sensor nodes rekeying process. Instead, multiple key controllers handle the key management process which is either dynamically assigned or predetermined. With this process, it enables better scalability of network and avoids a single point of failure.^{9, 31} These schemes are popularly categorized into three different schemes:

EBS Scheme

refers to a conjunctive formulation of key management problems in WSN system. Consisting of Γ subsets of nodes set, the EBS system generate optimal key set of k , m , and n parameters wherein k represents number of keys stored in member node (Each), m is rekeying messages number, and n is group size. This distributed key management scheme consist of SHELL, LOCK, Batch rekeying, and MUQAMI+ schemes. Disadvantage of using these schemes is that with low resilience even if small nodes in network are compromised, entire network information could be uncovered by adversary.^{31, 37}

PCGR Based Scheme

belong to collaboration-based and pre-distribution group of rekeying which are mainly proposed for providing solution to node compromise. Herein sensor nodes are assigned to several groups randomly, and each group has a unique key.

Consisting of mainly B-PCGR, C-PCGR, cluster-based, and compromise resilient, these schemes have high robustness in node capture attacks compared to EBS schemes.^{9, 31}

Deterministic Sequence Number-Based Schemes

this scheme, overcoming the vulnerability towards DoS attacks and resource exhausting attacks, is developed to maintain and securely establish local cluster and pairwise keys. This scheme is not dependent on infrastructures like base station or robots. It also does not require a single node for sharing master key and makes the functioning more flexible, thus supporting the enhancement of message security in data transmission and key update.^{31, 38}

Despite its relevance, distributed key management scheme is prone to design errors as compromised sensor codes find inclusion even in the node eviction process. They offer the flexibility of making relevant changes and are not dependent on central key controller.³⁹ Distributed key management schemes tend to support the functionality of HWSN and enable better results computation.⁹

Centralized Dynamic Key Management Schemes

Centralized dynamic key management schemes use single central key controller like third party or base station for the replacement and management of key materials of network nodes.³³ Herein, compromised sensor nodes are unable to sabotage node eviction process. Distributing or revoking cryptographic keys are faster in distributed key management schemes due to their broadcasting only with few hops but centralized system require multi-hops process for transmission of information from central key controller to specific sensor nodes.⁹ Some systems include:

- Genetic Algorithms Wherein Key Generating Function Can Be Encoded As Chromosomes Which Are Responsible For Selecting Low Power Consumption Constraints And Having Relative High Fitness Value Derivation,⁴⁰
- Public Key Cryptography Based Algorithm Wherein The Gateway Could Be Tamper Resistant And Less Resource Constraint,⁴¹ And
- One-Way Hash Chain Based Forward Authentication Key Management Scheme Consisting Of Base Station, High End Sensors

And Low-End Sensors Wherein With Discovery Of Compromised Node By Base Station, The Revocation Message Is Broadcasted To High End Sensors And Forwarded It To Low End Sensors For Removing Compromised Nodes Id. After Usage Of Last Key And With Sufficient Power By High End Sensor, New Key Chain Is Created.⁴²

Thus, though centralized key management schemes enable data transmission, due to their limitation in flexibility, central key controller, difficulty in information transmission, and less efficient resource and energy utilization, they are less preferred for HWSN systems.⁹

Security Analysis and Performance Evaluation

The performance and security analysis of key management schemes enables the comparison of the efficiency, flexibility, scalability, resilience, security, and mobility of the schemes in order to facilitate the identification of the optimal key management scheme for a specific scenario.²⁹

Examination of the performance is categorized into 3 parts: communication pass, message size, computation overhead, memory consumption, and energy consumption.⁴³ Security analysis is performed by assessing the respective key management scheme on the scale of sensor node authentication, confidentiality and message authentication, forward and backward secrecy, resilience, security against known attacks, and collusion resistance.¹⁰ The effectiveness of a sensor node depends on examination of the nature of communication between the nodes, size of messages supported by the node for transmission, cryptography and authentication methods associated computation overhead, or the amount of energy consumed by HWSN in their process. Further, the security analysis determines the capability of a key management scheme to prevent the damage from attacks and have the security management in the process of data transmission. Thus, based on the depth of data from a respective field, the performance and security analysis is done to determine appropriate key management scheme for HWSN system.^{7, 10}

Table 1: Comparison of dynamic key management schemes^{31, 44}

Type	Scheme	Node Revocation	Forward and Backward Secrecy	Collusion Resistance	Scalability	Key Connectivity
EBS	SHELL	Compromised CH revoke by cluster reorganization or non-CH node revoke locally	Both	partial	low	probability of two nodes sharing key like p1
	LOCK	Compromised CH revoke by BS or non-CH node revoke locally	Both	partial	medium	probability of two nodes sharing key like p2
PCGR	B-PCGR	group key revoke	Backward	most μ	high	100%
	C-PCGR	group key revoke	Backward	most μ	high	100%
	Cluster-based	For compromised node remove hierarchial key and group key revoke	Both	most t	high	100%
	Compromise -resilient		N.A.	Both	Yes	N.A 100%

Between distributed and centralized schemes, distributed dynamic key management schemes are

more effective source of data transmission. Among them, the deterministic sequence number-based

scheme are flexible scheme with high resilience and mobility support but costly while PCGR are efficient schemes with high resilience and high scalability. Centralized schemes are less flexible, less efficient, and limit the data transmission process; however, among these schemes, one-way hash chain is tend to be most effective with robustness to various attacks like replay attacks or guessing attacks.

Conclusion and Future Scope

Security has always been a challenging issue in WSN systems. Although with time various developments have taken place to create new key management schemes for enhancing security, data transmission process, and better results computation, efficiency of the data and the security from various known and unknown attacks have persistently been an issue. For overcoming these limitations of WSN systems, establishment of cryptographic keys is a primary area of concern. Studies have shifted towards exploration of key management scheme aspect in WSN systems with less focus on dynamic key management schemes. Since static cryptographic keys remain same throughout sensor nodes lifetime, they lack in aspect of flexibility and tackling attacks. Thus, this paper aimed at examining the dynamic key management schemes for the heterogeneous wireless sensor network system.

It was found that with the presence of link, computational, and energy heterogeneity, the HWSN system contributes to decreasing latency of data transportation, improving reliability in data transmission process, and prolonging network lifetime. This enables their wider applications in

the tasks like monitoring, localization, or even detection. The dynamic key management scheme selected for a particular HWSN system meeting the efficiency, flexibility, and security metrics tend to help in resolving problem associated with maintenance, distribution, and generation of secret keys. Various dynamic key management schemes like SHELL, Basic scheme, SKM, or hybrid scheme based on storage can be broadly be divided into two categories i.e. distributed and centralized schemes. Efficient key management scheme for the HWSN system nodes include better performance and security structure of distributed schemes, the keys like EDDK, Cluster-based, or compromise resilient.

This study is limited to the identification of the efficient key management schemes. Future researches can explore the security and resistance of the respective schemes in presence of captured attacks to have practical examination of the efficiency. Further, focusing on the criteria of performance and security analysis, future studies can present more detailed examination of the centralized dynamic key management schemes and determining the aspects which limits its efficiency against distributed dynamic key management schemes.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Conflict of Interest

The authors do not have any conflict of interest.

References

1. S. Seo, J. Won, S. Sultana, and E. Bertino, "Effective Key Management in Dynamic Wireless sensor networks," *Cyber Cent. Publ.*, vol. 10, no. 2, pp. 371–383, 2015.
2. A. S. K. Pathan, C. S. Hong, and H. W. Lee, "Smartening the environment using wireless sensor networks in a developing country," in *8th International Conference Advanced Communication Technology, ICACT 2006 - Proceedings, 2006*, vol. 1, pp. 705–709, doi: 10.1109/icact.2006.206063.
3. U. B. Desai, B. N. Jain, and S. N. Merchant, "Wireless Sensor Networks : Technology Roadmap," 2007. [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.458.8531&rep=rep1&type=pdf>.
4. H.-W. Lee, C. S. Hong, and A.-S. K. Pathan, "Security in Wireless Sensor Networks: Issues and Challenges," 2006.
5. T. Zia and A. Zomaya, "Security Issues in Wireless Sensor Networks," 2006.
6. V. Kumar, A. Jain, and P. Barwal, "Wireless Sensor Networks: Security Issues, Challenges and Solutions," *Int. J. Inf. Comput. Technol.*, vol.

- 4, no. 8, pp. 859–868, 2014.
7. E. Bai and X. Jiang, "A dynamic key management scheme based on double key for wireless sensor networks," *Telkomnika*, vol. 11, no. 3, pp. 1514–1523, 2013.
 8. S. Athmani, A. Bilami, and D. E. Boubiche, "EDAK: An Efficient Dynamic Authentication and Key Management Mechanism for heterogeneous WSNs," *Futur. Gener. Comput. Syst.*, 2017, doi: 10.1016/j.future.2017.10.026.
 9. X. He, M. Niedermeier, and H. De Meer, "Dynamic key management in wireless sensor networks: A survey," *J. Netw. Comput. Appl.*, vol. 36, no. 2, pp. 611–622, 2012, doi: 10.1016/j.jnca.2012.12.010.
 10. S. H. Erfani, H. H. S. Javadi, and A. M. Rahmani, "A dynamic key management scheme for dynamic wireless sensor networks," *Secur. Commun. Networks*, vol. 8, no. 6, pp. 1040–1049, 2015, doi: 10.1002/sec.1058.
 11. C. M. Chen, X. Zheng, and T. Y. Wu, "A complete hierarchical key management scheme for heterogeneous wireless sensor networks," *Sci. World J.*, vol. 2014, 2014, doi: 10.1155/2014/816549.
 12. A. Pattanaik and B. Majhi, "Weakness of Key Predistribution Scheme Proposed by J. Dong et al.," *IACR Cryptol*, vol. 114, no. ePrint Arch., 2009.
 13. D. E. Boubiche, S. Athmani, S. Boubiche, and H. Toral-Cruz, "Cybersecurity Issues in Wireless Sensor Networks: Current Challenges and Solutions," *Wirel. Pers. Commun.*, 2020, doi: <https://doi.org/10.1007/s11277-020-07213-5>.
 14. K. Kifayat, M. Merabti, Q. Shi, and D. Llewellyn-Jones, *Security in Wireless Sensor Networks*. Berlin: Springer, 2010.
 15. E. Walid, T. Newe, M. Fraifer, and E. O'Connell, "Implementing Secure Key Coordination Scheme for Line Topology Wireless Sensor Networks," in *Advances in Security in Computing and Communications*, 2017.
 16. S. A. Camtepe and B. Yener, "Key management in wireless sensor networks," *Inf. Secur. J.*, 2008, doi: 10.1080/19393555.2019.1628326.
 17. M. R. Alagheband and M. R. Aref, "A secure key management framework for heterogeneous wireless sensor networks," vol. 7025 LNCS, pp. 18–31, 2011, doi: 10.1007/978-3-642-24712-5_2.
 18. R. K. Kodali, S. Chougule, and A. Agarwal, "Key management technique for heterogeneous wireless sensor networks," *IEEE 2013 Tencon - Spring, TENCONSpring 2013 - Conf. Proc.*, pp. 183–187, 2013, doi: 10.1109/TENCONSpring.2013.6584437.
 19. A. S. Elqusy, S. E. Essa, and A. El-Sayed, "A Key Management Techniques in Wireless Sensor Networks," *Commun. Appl. Electron.*, vol. 7, no. 2, pp. 8–18, 2017, doi: 10.5120/cae2017652600.
 20. S. V. Manikanthan and T. Padmapriya, "A secured multi-level key management technique for intensified wireless sensor network," *Int. J. Recent Technol. Eng.*, vol. 7, no. 6, pp. 544–551, 2019.
 21. E. Yuan, L. Wang, S. Cheng, N. Ao, and Q. Guo, "A Key Management Scheme Based on Pairing-Free Identity Based Digital Signature Algorithm for Heterogeneous Wireless Sensor Networks," *Sensors*, 2020.
 22. A. B. Kalyani, "Heterogeneous Network Framework Architecture – A Survey," *Int. J. Comput. Sci. Inf. Technol. Secur.*, vol. 2, no. 4, pp. 869–874, 2012.
 23. G. Wagenknecht, M. Anwander, T. Braun, T. Staub, J. Matheka, and S. Morgenthaler, "MARWIS: A management architecture for heterogeneous wireless sensor networks," vol. 5031 LNCS, no. January, pp. 177–188, 2008, doi: 10.1007/978-3-540-68807-5_15.
 24. M. R. Dhage and S. Vemuru, "Routing design issues in heterogeneous wireless sensor network," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 2, pp. 1028–1039, 2018, doi: 10.11591/ijece.v8i2.pp1028-1039.
 25. M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting heterogeneity in sensor networks," in *Proceedings - IEEE INFOCOM*, 2005, vol. 2, pp. 878–890, doi: 10.1109/infcom.2005.1498318.
 26. J. J. Lee, B. Krishnamachari, and C. C. J. Kuo, "Impact of heterogeneous deployment on lifetime sensing coverage in sensor networks," in *2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, IEEE SECON 2004*, 2004, no. March 2016, pp. 367–376, doi: 10.1109/sahcn.2004.1381938.
 27. S. Mahajan and J. Malhotra, "Energy Efficient Control Strategies in Heterogeneous Wireless Sensor Networks: A Survey," *Int. J. Comput.*

- Appl.*, vol. 14, no. 6, pp. 31–37, 2011, doi: 10.5120/1886-2503.
28. Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Comput. Commun.*, vol. 30, no. 11–12, pp. 2314–2341, 2007, doi: 10.1016/j.comcom.2007.04.009.
 29. P. Ahlawat, "Key Distribution and Management in WSN Security: A State of the Art," *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 2S, pp. 462–472, 2019, doi: 10.35940/ijitee.b1118.1292s19.
 30. W. Z. Khan, N. M. Saad, and M. Y. Aalsalem, "An overview of evaluation metrics for routing protocols in wireless sensor networks," in *ICIAS 2012 - 2012 4th International Conference on Intelligent and Advanced Systems: A Conference of World Engineering, Science and Technology Congress (ESTCON) - Conference Proceedings, 2012*, vol. 2, pp. 588–593, doi: 10.1109/ICIAS.2012.6306083.
 31. S. R. Nabavi and S. M. Mousavi, "A Review of Distributed Dynamic Key Management Schemes in Wireless Sensor Networks," *J. Comput.*, vol. 13, no. 1, pp. 77–89, 2018, doi: 10.17706/jcp.13.1.77-89.
 32. R. Divya and T. Thirumurugan, "A Novel Dynamic Key Management Scheme Based On Hamming Distance for Wireless Sensor Networks," *Int. J. Sci. Eng. Res.*, vol. 2, no. 5, 2011.
 33. M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic key management in sensor networks," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 122–130, 2006, doi: 10.1109/MCOM.2006.1632659.
 34. X. Du, Y. Xiao, M. Guizani, and H. H. Chen, "An effective key management scheme for heterogeneous sensor networks," *Ad Hoc Networks*, vol. 5, no. 1, pp. 24–34, 2007, doi: 10.1016/j.adhoc.2006.05.012.
 35. N. Nisha and M. Dave, "Storage as a parameter for classifying dynamic key management schemes proposed for WSNs," in *2016 International Conference on Computational Techniques in Information and Communication Technologies, ICCTICT 2016 - Proceedings, 2016*, pp. 51–56, doi: 10.1109/ICCTICT.2016.7514551.
 36. A. K. Gautam and R. Kumar, "A comparative study of recently proposed key management schemes in wireless sensor network," in *2018 International Conference on Computing, Power and Communication Technologies, GUCON 2018, 2018*, pp. 512–517, doi: 10.1109/GUCON.2018.8674948.
 37. R. Jiang, J. Luo, F. Tu, and J. Zhong, "LEP: A lightweight key management scheme based on ebs and polynomial for wireless sensor networks," in *2011 IEEE International Conference on Signal Processing, Communications and Computing, ICSPCC 2011, 2011*, no. December, doi: 10.1109/ICSPCC.2011.6061682.
 38. X. Zhang, J. He, and Q. Wei, "EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks," *Eurasip J. Wirel. Commun. Netw.*, vol. 2011, 2011, doi: 10.1155/2011/765143.
 39. R. Seetha and S. Ramakrishnan, "A Survey on Group Key Management Schemes," *Cybern. Inf. Technol.*, vol. 15, no. 3, 2015.
 40. C. L. Wang, T. P. Hong, G. Horng, and W. H. Wang, "A ga-based key-management scheme in hierarchical wireless sensor networks," *Int. J. Innov. Comput. Inf. Control*, vol. 5, no. 12, pp. 4693–4702, 2009.
 41. M. H. Eldefrawy, M. K. Khan, and K. Alghathbar, "A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography," *Proc. - 2010 Int. Conf. Anti-Counterfeiting, Secur. Identification, 2010 ASID*, pp. 1–6, 2010, doi: 10.1109/ICASID.2010.5551480.
 42. I. E. Liao, J. Y. Huang, and H. W. Tang, "A forward authentication key management scheme for heterogeneous sensor networks," *Eurasip J. Wirel. Commun. Netw.*, vol. 2011, 2011, doi: 10.1155/2011/296704.
 43. W. Tiberti, F. Caruso, and L. Pomante, "Development of an extended topology-based lightweight cryptographic scheme for IEEE 802.15.4 wireless sensor networks," *Int. J. Distrib. Sens. Networks*, vol. 16, no. 10, 2020.
 44. R. Shaik and S. S. Ahamad, "Key management schemes of wireless sensor networks -a survey," *Fronteiras*, vol. 6, no. 2, pp. 526–537, 2017, doi: 10.21664/2238-8869.2017v6i2.p526-537.