**International Journal of Electrical Engineering and Technology (IJEET)**
Volume 11, Issue 10, December 2020, pp. 460-469, Article ID: IJEET_11_10_057
Available online at https://iaeme.com/Home/issue/IJEET?Volume=11&Issue=10
ISSN Print: 0976-6545 and ISSN Online: 0976-6553
DOI: https://doi.org/10.34218/IJEET.11.10.2020.057

# HYBRID KEY DISTRIBUTION AND MANAGEMENT SYSTEM FOR WIRELESS SENSOR NETWORKS

**Dr R. Sujatha**

Assistant Professor & Head, Department of Computer Science, Queens College of Arts and Science for Women (Affiliated to Bharathidasan University, Tiruchirappalli),
Punalkulam, Pudukkottai, Tamil Nadu, India

## ABSTRACT

*The majority of key management techniques ignore the adversary's attacking behaviour, making them less practical in the real world. The defender/network designer can effectively and efficiently construct many countermeasures against hostile behaviour by understanding it. The problem of compromise link is investigated in this research, and a secure Hybrid Key Pre-Distribution strategy (HKPS) for wireless sensor networks is proposed (WSN). The robustness of the q-composite system is combined with the threshold resistant polynomial technique in this approach. The suggested approach intends to strengthen the network's resilience to node capture attacks.*

**Key words:** Key Pre-distribution, Wireless Sensor Network, Security Services, Attack probability, q-Composite scheme, Resilience against node capture, Key connectivity, Random key pre-distribution scheme.

**Cite this Article:** R. Sujatha, Hybrid Key Distribution and Management System for Wireless Sensor Networks, *International Journal of Electrical Engineering and Technology (IJEET).* 11(10), 2020, pp. 460-469.
https://iaeme.com/Home/issue/IJEET?Volume=11&Issue=10

## 1. INTRODUCTION

The Wireless Sensor Network (WSN) is made up of small sensors with limited resources that actively monitor their surroundings, gather data, and transfer it to a central authority. The Base Station (BS) serves as the central authority and serves as a strong data processing and storage facility [1]. Because the sensors' energy and processing power are restricted, heavy-weight public key encryption is an impractical solution for WSN security. For WSN, security methods should be light and energy-efficient. One strategy for reducing energy consumption during query processing is duty cycled WSNs, in which sensors sleep and wake up at regular intervals. Another strategy for improving the energy efficiency of WSNs coupled with mobile cloud computing is location-based sleep scheduling [2]. WSNs are vulnerable to a variety of threats because to their low resources and deployment in dangerous locations. The node capture assault is an example of such an attack. The resistance of the Key Management Scheme (KMS) to this attack has emerged as a critical and difficult issue in WSN security. The security of the WSN is based on the keys used to encrypt the data [3] [4]. As a result, the primary concern is how to build a secure KMS that ensures proper WSN service operation even in the face of an adversary [5]. WSNs are used in a variety of fields, including defence, medical care, environmental monitoring, disaster management, and inventory control. KMS is a series of mechanisms that make data transmission between sensor nodes more secure [6].

Because of the wireless nature of the communication channel, WSN has various inherent security vulnerabilities such as eavesdropping, forgery attacks, and off-line guessing attacks. These networks are frequently deployed in unmanaged, hostile, and vital situations, necessitating the use of effective and efficient security solutions. To sustain continuous relationships in a network, key establishment systems strive to supply pair-wise keys among surrounding nodes. However, because to the restricted processing power, battery power, and storage capacity of sensor nodes, it becomes complex. The majority of KMS assumes that every node in the network has the same attack probability. Many WSN uses, such as military and border monitoring, may not be true, making these systems less viable in real-world situations. Is it possible to create procedures that strengthen the resilience and connection of critical pre-distribution schemes? "A system without opponent definition cannot be secure," it was also stated. [7] says, "It can only be amazing." It states that defensive systems should be created after a thorough examination of the adversary's conduct. An attack like node capture would not be able to decrease the performance of KMS to such a degree if there was a reliable, secure, and realistically constructed KMS for WSNs. Motivated by this fact, this study proposes an attack-resistant key pre-distribution scheme that combines the strengths of the q-composite and the polynomial scheme to strengthen the network's resistance to node capture.

## 2. LITERATURE REVIEW

WSNs are vulnerable to a variety of attacks due to their intrinsic characteristics. These attacks compromise the network's confidentiality, integrity, and availability. Passive and aggressive attacks are two types of such attacks. Passive attacks such as eavesdropping, traffic analysis, and passive monitoring involve unauthorized people listening in on communication channels. These attacks compromise the network's data's confidentiality and privacy. Active attacks in the network falsify, manipulate, listen to, and monitor data packets. Camouflage, sybil, wormhole, replay, hello flood, sink hole, denial of service, and node replication are some of the most popular active attacks. Sink is the most trusted component of the WSN, and it cannot be hacked. Sink hole node identification is critical in WSN security because it operates as a conduit for forwarding gathered data to an external environment [8]. Even some threats, such as black holes, are difficult to detect and counter, therefore early detection and prevention are critical in network security [9] [20] [21]. Authentication is also an important part of security since it provides authorized access to data collected by sensor nodes [10] [22] [23] [24] [25].

The key distribution strategies in WSN security were the subject of this paper. By ensuring secure communication among the sensor nodes, KMS plays a critical function. For WSNs, the authors developed a random key pre-distribution mechanism [5]. This plan is also known as the EG scheme or the fundamental scheme. It is divided into three phases: key pre-distribution, shared key discovery, and path key establishment. A big key pool is used to assign the keys. If the nodes are unable to locate a common key, they use intermediate nodes to build a path key. The q-composite system, in which nodes must share q keys instead of one, reinforced the EG scheme [11]. This improves the scheme's security. A deployment-based key management strategy is presented [12], in which adjacent nodes in a network share a greater number of keys than non-neighboring nodes. The need for prior deployment knowledge restricts their practical application. The authors [6] describe a secure approach that takes into account dangers that may arise within the network. The pair-wise key is established using bivariate polynomials in a polynomial pool scheme [13]. Although this approach has a considerable storage overhead, it provides great security in small-scale attacks. The t-threshold property of the polynomial scheme asserts that if the number of captured nodes is smaller than t, the scheme is not compromised. Many experts have recently proposed a combination strategy that incorporates the benefits of two different approaches while maintaining a low level of complexity. Authors [14] proposed a hash-based key pre-distribution approach for WSN in [15]. The hash function is employed to keep the pre-distributed keys hidden from prying eyes. This approach has been demonstrated to be more resistant against node capture. [12] proposes an uneven key distribution strategy in which high-end sensors have larger key rings and low-end sensors have smaller key rings. KMS's overall performance improves as a result of the above.

## 3. PROPOSED HYBRID KEY PRE-DISTRIBUTION SCHEME

The network designer or defender first creates an attack matrix by examining various vulnerabilities. This matrix is created by taking the adversary's point of view into account when the nodes in the network are deployed. An attacker has complete knowledge of the network topology, routes, and key identifiers [16] [17] [18] [19]. An attack is formalised using this matrix, and a collection of captured candidate nodes is calculated. The network's nodes are divided into two categories: vulnerable and safe nodes. When compared to secure nodes, vulnerable nodes are given smaller key rings. Because the number of stored keys is modest, the risks of key compromise are minimised, increasing the resilience of the suggested method. The smaller key ring decreases the risk of keying information being leaked to the enemy. The hash chaining of a node's pre-distributed keys is performed using the node's attack coefficient.

**Table 1** Algorithm Notation and its meaning

| Notation | Meaning |
|---|---|
| N | Total nodes of the network |
| C | Set of cut vertex node |
| $K_j$ | Keys contained by $j^{th}$ node |
| $AAC_i$ | Application attack coefficient of ith node |
| S | Set of sink nodes |
| $ac_i$ | Attack coefficient of ith node |
| $CC_i$ | Capturing cost of ith node |
| $C_n$ | Set of compromised nodes |
| $C_k$ | Set of compromised keys |
| $ID_v$ | Node identifier |
| M | Key ring size |
| P | Key pool |
| L | Limit parameter |
| N | Polynomial shares |
| P | Polynomial pool |
| CVD | Matrix based on Cut Vertex |
| AC_CVD | attack coefficient of a nodes based CVD matrix |
| CVP | cut vertex partial compromise matrix |
| AC_CVP | attack coefficient based CVP matrix |
| SD | matrix based on the direct sink key compromise |
| AC_SD | attack coefficients of the nodes based on the sink node |
| SP | partial compromise of the nodes with sink node |
| AC_SP | attack coefficient based on SP |
| A_CD | attack coefficient based on direct compromise |

| | |
|---|---|
| CP | attack coefficient based on partial compromise |
| AC_D | attack coefficient based on direct compromise |
| AC_P | attack coefficient based on partial compromise |
| F’AC | final value of the attack coefficient of the node based on the capturing cost |
| CC | Cost of capturing a sensor node |
| cmd | relative importance of the direct compromise over partial compromise |
| d | number of sink nodes |
| k | hop distance from the sink |
| lp | limit parameter |
| $sk_t$ | the number of sub key pools |
| $skp_k$ | each sub key pool has number of keys |
| v | sub key pool of a node |
| $ID_{Kp(v)}$ | each key with a sub key pool identifier list |

## Algorithm: Hybrid Key Pre-distribution Scheme

***Step 1:*** Method 1: To compute attack coefficient of a node based on node dominance (AC-ND)

*Step 1.1:* Input: N, K, S, SR

*Step 1.2:* Output: DC, PC

*Step 1.3:* for all $n_i \in N-(S + SR)$

*Step 1.4:* for all $n_j \in N-(S + SR)$

*Step 1.5:* if $n_i$ can directly compromise $n_j$ $dc_{ni}^{++}$

*Step 1.6:* else if $n_i$ can partially compromise $n_j$ $pc_{ni}^{++}$

*Step 1.7:* end if

*Step 1.8:* end if

*Step 1.9:* end for

*Step 1.10:* end for

*Step 1.11:* end for

*Step 1.12:* return DC and PC // Return the attack coefficient of a node

***Step 2:*** Method 2: To identify the set of candidate capture node based on estimated value of F’AC

*Step 2.1*. Input: AC_D, AC_P, cmd

*Step 2.2*. Output: $C_n$ and $C_k$/*$C_n$ is the set of compromised nodes and $C_k$ is the set of compromised keys*/

*Step 2.3*: Construct FAC

*Step 2.4:* Construct CC

*Step 2.5:* Construct F’AC

*Step 2.6:* while all routing paths are destroyed do

*Step 2.7:* Find $n_i \in V$ such that it has maximum attack coefficient i.e. $C_n \in \arg\max$ (F’AC)

*Step 2.8:* Select $n_i$, $C_n = C_n \cup n_i$, $C_k = C_k \cup k_i$

*Step 2.9:* Adjust F’AC

*Step 2.10:* end while

*Step 2.11:* return $C_n$ and $C_k$

***Step 3:*** Method 3: To assign a random key to the nodes in the proposed scheme.

*Step 3.1:* Input: $ID_v$ ,. . .,$ID_{Kr(v)}$; $ac_{(u)}$, Hash function, lp

*Step 3.2:* Output $ID_{Kr(v)}$, KP(v) KDS randomly group the keys into $sk_t$ key pools where each sub key pool has $skp_k$ keys

*Step 3.3:* KDS assigns $sk_n$ key pool to each node of the network

*Step 3.4:* r number of keys from each sub key pool are randomly assigned to the nodes

*Step 3.5:* For $n_i \in N$ $kr_i$ = {$hash^{acimodlp}$ ($k_1$), $hash^{acimodlp}$ ($k_2$) . . . $hash^{acimodlp}$ ($k_r$)}

*Step 3.6:* return $ID_{Kr(v)}$, KP(v)

## 4. PERFORMANCE ANALYSIS OF THE PROPOSED HYBRID KEY PRE-DISTRIBUTION SCHEME

### 4.1. Polynomial and Key Connectivity

The likelihood that two nodes in a communication range have the same key is known as key connectivity. Even if we store fewer keys in susceptible nodes in the HKP scheme, as shown in Fig. 1, the key connectivity stays the same. M x N = x2 is the relationship between the two pre-distribution techniques' polynomial rings. We also notice that even if only a small percentage of polynomial shares are stored in vulnerable nodes in the proposed scheme, the key connectivity remains the same as in a balanced distribution. This is because the total polynomial shares in both schemes are the same. This demonstrates the efficacy of the suggested strategy in terms of enhanced security without compromising vital connectivity. We also notice that as the polynomial size grows, the key connectivity diminishes. We used the following variables to plot this figure: key ring size of nodes in balanced key pre-distribution s = [2, 4], key ring size of safe nodes in proposed scheme m = [4, 8], and key ring size of vulnerable nodes in proposed scheme n = [1, 2].

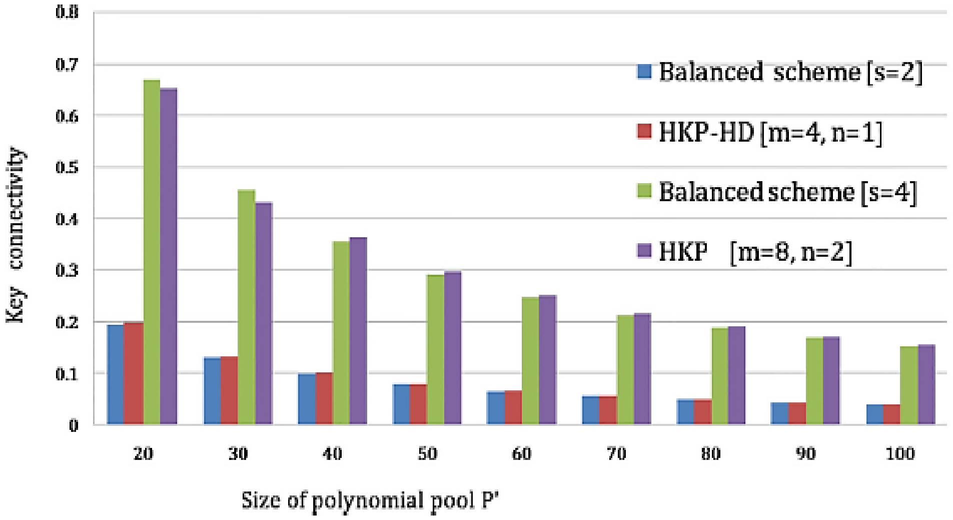

**Figure 1** The relationship between the polynomial pool size and the key connectivity

### 4.2. Probability of key Compromise

In comparison to other existing schemes, the HKPS has the lowest probability of key compromise (see Figure 2). PPBR stands for polynomial pool with key pool system, while Du stands for uneven key pre-distribution. The size of the key ring in the PPBR system is obviously smaller than in the Du design. As a result, the PPBR key ring size is smaller, resulting in a lower probability of key compromise than the Du system. The projected HKP-HD has an even lower chance of key compromise than the PPBR. It's because hash chain pre-distribution with several sub key pools is used. As a result, the proposed HKP scheme reduces the PPBR system's key compromise likelihood even more. In the proposed HKP-HD, the chance of key compromise decreases when the value of q is increased, as shown in Fig. 2(a), 2(b), and 2(c). This is owing to the fact that when q rises, key overlapping rises with it. As a result, the number of captured nodes rises, making it easier to break the connection keys. The suggested scheme's hash-based pre-distribution reduces the likelihood of key compromise, and hence reduces the number of afflicted nodes during node capture. This raises the scheme's resilience to node capture even more. As the number of captured nodes approaches 100, the likelihood of key compromise approaches one, as the value of variable t is set to 100. S = 1000, t = 100, m = 40, P0 = 14, n = 5, lp = 10 are the values used to produce the graph: S = 1000, t = 100, m = 40, P0 = 14, n = 5, lp = 10.

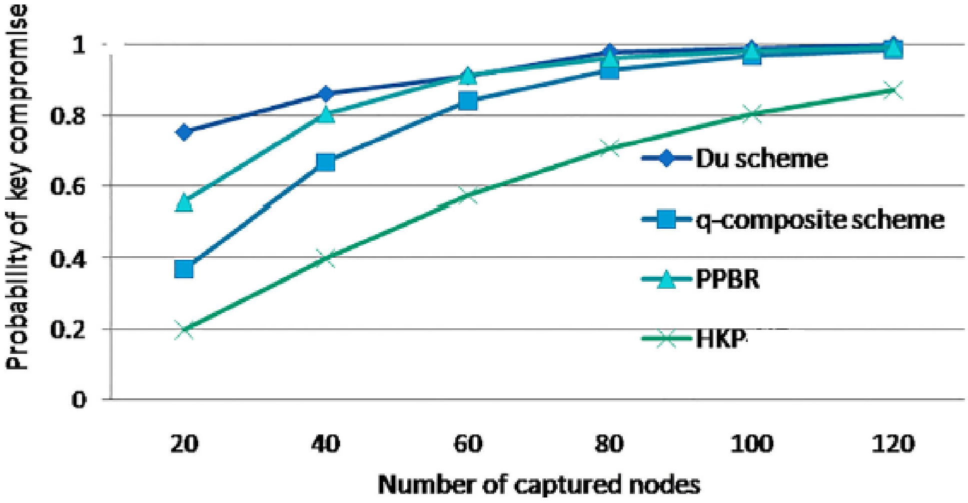

**Figure 2a** Probability of key compromise for number of captured nodes with q=1

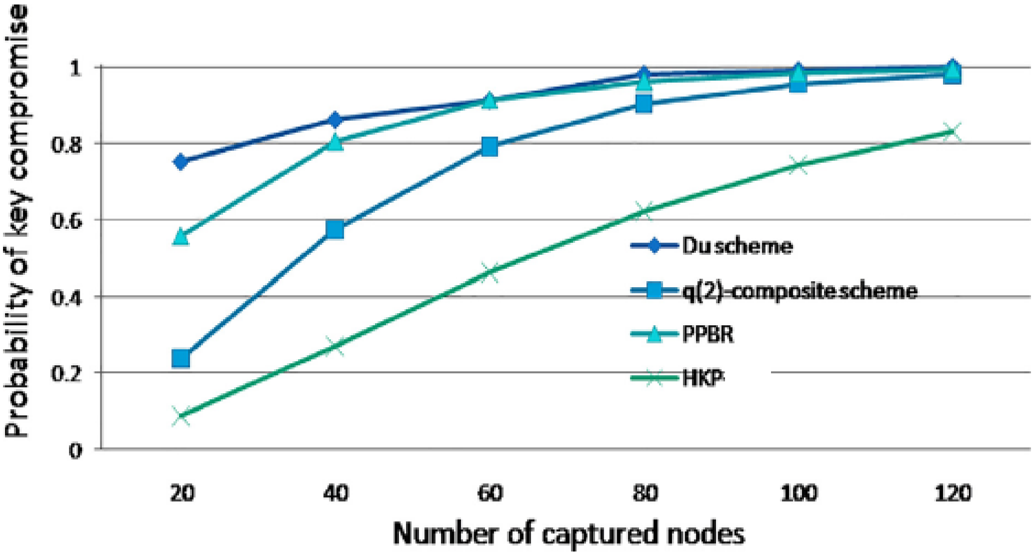

**Figure 2b** Probability of key compromise for number of captured nodes with q=2

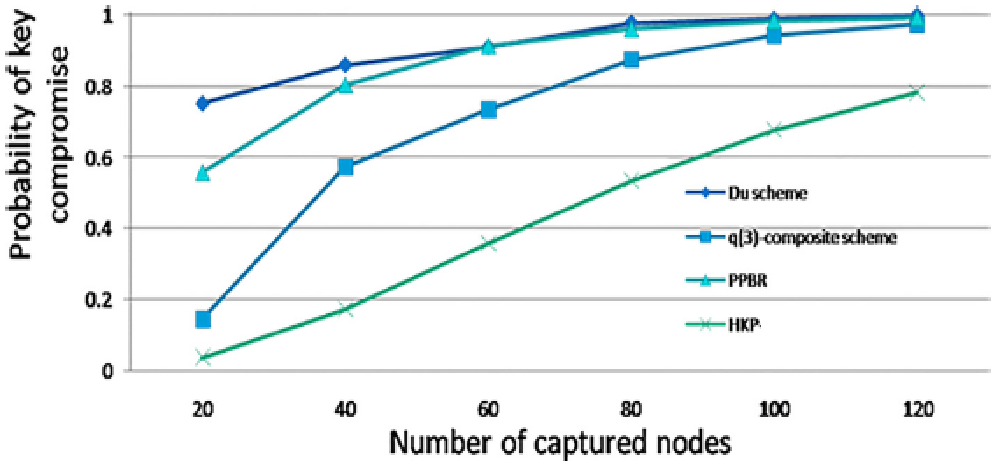

**Figure 2c** Probability of key compromise for number of captured nodes with q=3

## 4.3. Communication Overhead

As shown in Figures 3(a) and 3(b), the HKP scheme has the lowest communication overhead when compared to the Du scheme. The HKP system splits the domain key pool into subkey pools. The shared key is discovered in two steps in the HKP scheme. The sub key pool identifiers are transferred over a network in the first stage. Only when the communicating nodes share common key pool identifiers does the second stage begin. In the second stage of key discovery, the node broadcasts the key identifiers of shared sub key pools. During shared key discovery in the Du scheme, the key IDs are compared. When compared to the HKP scheme, this results in a significant number of key comparisons and consequently a higher communication overhead. When the size of the key pool is increased, the communication overhead in the Du method increases faster than in the proposed scheme. The same can be said for increasing the size of the key ring.

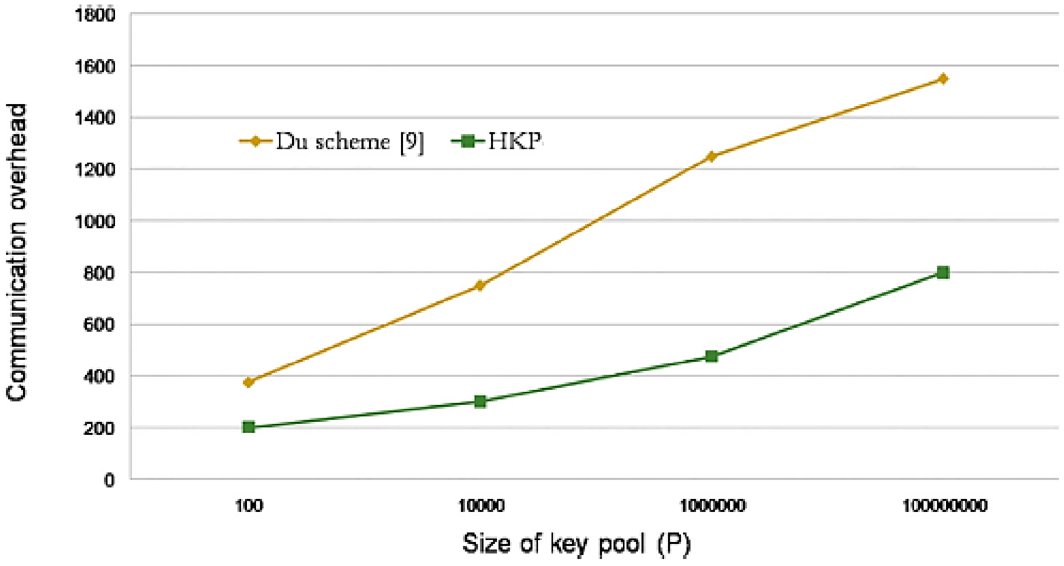

**Figure 3a** Comparison of the communication overhead with $k_{spn}$ >2

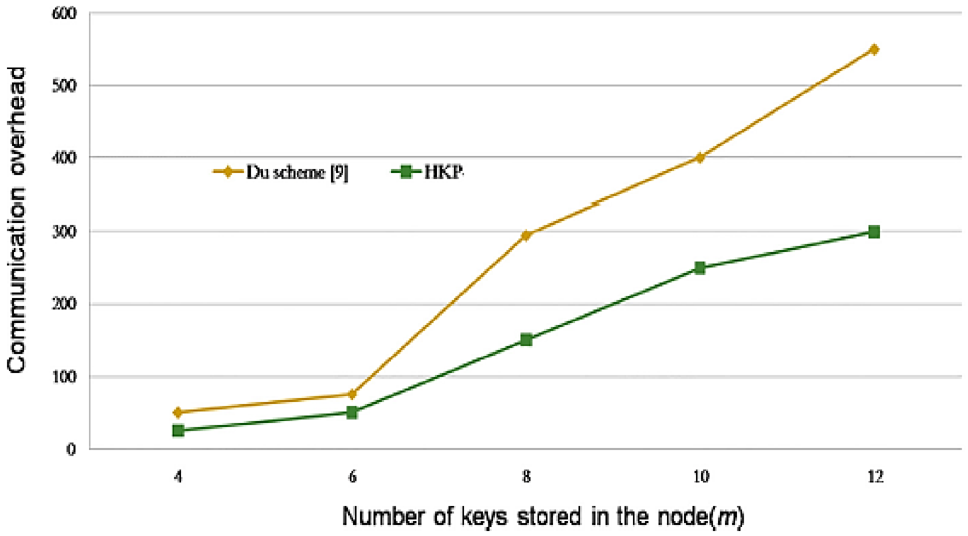

**Figure 3b** Comparison of the communication overhead with $k_{spn}$ = 2

## 5. CONCLUSION

This work proposesd an attack-resistant key pre-distribution (HKP) that combines the q-composite scheme's resilience with the polynomial pool scheme's unconditional secrecy. The suggested system is designed to reduce communication overhead and the likelihood of key compromise while maintaining critical connectivity. The proposed scheme's hash chain with numerous sub key pools minimised the likelihood of key compromise and communication overhead. The suggested scheme's imbalanced key pre-distribution reduces the storage overhead on the network's vulnerable nodes while maintaining key connectivity. It strengthens the proposed scheme's resistance to node capture.

## REFERENCES

[1] Akyildiz, Ian F., et al. "Wireless sensor networks: a survey." *Computer networks* 38.4 (2002): 393-422.

[2] Zhu, Chunsheng, et al. "Insights of Top-$ k $ Query in Duty-Cycled Wireless Sensor Networks." *IEEE Transactions on Industrial Electronics* 62.2 (2014): 1317-1328.

[3] Zhang, Junqi, and Vijay Varadharajan. "Wireless sensor network key management survey and taxonomy." *Journal of network and computer applications* 33.2 (2010): 63-75.

[4] Bhushan, Bharat, and Gadadhar Sahoo. "Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks." *Wireless Personal Communications* 98.2 (2018): 2037-2077.

[5] Eschenauer, Laurent, and Virgil D. Gligor. "A key-management scheme for distributed sensor networks." *Proceedings of the 9th ACM Conference on Computer and Communications Security*. 2002.

[6] Choi, Jaewoo, et al. "Location-based key management strong against insider threats in wireless sensor networks." *IEEE Systems Journal* 11.2 (2015): 494-502.

[7] Gligor, Virgil D. "Handling new adversaries in wireless ad-hoc networks (transcript of discussion)." *International Workshop on Security Protocols*. Springer, Berlin, Heidelberg, 2008.

[8] Wazid, Mohammad, et al. "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks." *Security and Communication Networks* 9.17 (2016): 4596-4614.

[9] Wazid, Mohammad, and Ashok Kumar Das. "A secure group-based blackhole node detection scheme for hierarchical wireless sensor networks." *Wireless Personal Communications* 94.3 (2017): 1165-1191.

[10] Wu, Fan, et al. "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment." *Journal of Network and Computer Applications* 89 (2017): 72-85.

[11] Chan, Haowen, Adrian Perrig, and Dawn Song. "Random key predistribution schemes for sensor networks." *2003 Symposium on Security and Privacy, 2003.*. IEEE, 2003.

[12] Du, Wenliang, et al. "A key management scheme for wireless sensor networks using deployment knowledge." *IEEE INFOCOM 2004*. Vol. 1. IEEE, 2004.

[13] Liu, Donggang, Peng Ning, and Wenliang Du. "Group-based key predistribution for wireless sensor networks." *ACM Transactions on Sensor Networks (TOSN)* 4.2 (2008): 1-30.

[14] Bechkit, Walid, Yacine Challal, and Abdelmadjid Bouabdallah. "A new class of Hash-Chain based key pre-distribution schemes for WSN." *Computer communications* 36.3 (2013): 243-255.

[15] Zhang, Jianmin, Qingmin Cui, and Rui Yang. "A Hybrid Key Establishment Scheme for Wireless Sensor Networks." *International Journal of Security and its applications* 10.2 (2016): 411-422.

[16] Lin, Chi, et al. "A low-cost node capture attack algorithm for wireless sensor networks." *International Journal of Communication Systems* 29.7 (2016): 1251-1268.

[17] Chen, Xiangqian, et al. "Attack DistributionModeling and Its Applications in Sensor Network Security." (2008).

[18] Yu, Chia-Mu, et al. "An application-driven attack probability-based deterministic pairwise key pre-distribution scheme for non-uniformly deployed sensor networks." *International Journal of Sensor Networks* 9.2 (2011): 89-106.

[19] Ahlawat, Priyanka, and Mayank Dave. "An improved hybrid key management scheme for wireless sensor networks." *2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*. IEEE, 2016.

[20] Subhashini, M., & Gopinath, R., Mapreduce Methodology for Elliptical Curve Discrete Logarithmic Problems – Securing Telecom Networks, International Journal of Electrical Engineering and Technology, 11(9), 261-273 (2020).

[21] Upendran, V., & Gopinath, R., Feature Selection based on Multicriteria Decision Making for Intrusion Detection System, International Journal of Electrical Engineering and Technology, 11(5), 217-226 (2020).

[22] Upendran, V., & Gopinath, R., Optimization based Classification Technique for Intrusion Detection System, International Journal of Advanced Research in Engineering and Technology, 11(9), 1255-1262 (2020).

[23] Subhashini, M., & Gopinath, R., Employee Attrition Prediction in Industry using Machine Learning Techniques, International Journal of Advanced Research in Engineering and Technology, 11(12), 3329-3341 (2020).

[24] Rethinavalli, S., & Gopinath, R., Classification Approach based Sybil Node Detection in Mobile Ad Hoc Networks, International Journal of Advanced Research in Engineering and Technology, 11(12), 3348-3356 (2020).

[25] Rethinavalli, S., & Gopinath, R., Botnet Attack Detection in Internet of Things using Optimization Techniques, International Journal of Electrical Engineering and Technology, 11(10), 412-420 (2020).