International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Optimization of Keys Using Grey-Wolf Optimization for Secure Path Key Establishment Schemes in Wireless Sensor Networks

Girija Vani Gurram[1]* **Noorullah Shariff Chowdary[2]** **Rajkumar Laxmikanth Biradar[3]**

[1]*Department of Electronics and Communication Engineering,*
Rao Bahadur Y Mahabaleswarappa Engineering College, Ballari, India
[2]*Department of Electronics and Communication Engineering,*
SECAB Institute of Engineering & Technology, Vijayapur, India
[3]*Department of Electronics and Telematics Engineering,*
G. Narayanamma Institute of Technology and Science, Hyderabad, India
* Corresponding author's Email: vanigirijag@gmail.com

Abstract: Security of Wireless Sensor Node (WSN) is an important issue due to inherited nature and uncontrolled operation, which makes it vulnerable to many attacks Sybil attacks, denial of service attacks, etc. The main issue related to WSN is the key management system, as it plays an important role in providing security services for WSNs. However, developing a distribution/establishment scheme for WSNs is challenging due to limited sensor sources. In this study, three schemes namely proxy-based path key establishment (PPK), friend-based path key establishment (FPK) and disjoint path key establishment (DPK) are developed. The main problem of path key explore is minimized by passing the nodes with high value of attack coefficient. In PPK model, the Grey-Wolf Optimization (GWO) is used to optimize the threshold value for k-key fragment number and categorization of nodes. The nodes having the common key with destinations are identified by FPK and the best path to reach the destinations is selected by DPK. According to the path compromise ratio and probability of key recovery, the resistance to the effectiveness of three proposed schemes are verified. The results proved that the proposed PPK-GWO achieved probability of key recovery 0.8 for 100 captured nodes, where the DPK achieved the probability of path compromise 0.95 for 10 captured nodes.

Keywords: Grey-wolf optimization, Key establishment scheme, Path key explore, Security, Sybil attacks, Wireless sensor network.

1. Introduction

WSN comprises a plethora of tiny sensor nodes, with limited resources dedicated to various surveillance applications in an unsecure environment. Generally, unsecure WSN networks are easy for the adversaries to launch attacks and compromise the nodes. If the right chord struck, it harms the entire network. The WSN nodes with restricted resources barely confront the hostilities posed by the adversaries in operative environment. With such attacks, the adversary searches the site and steals secret keying information then provides a secure communication for WSN [1]. The Key Management scheme (KMS) delivers secure communications among the adversary's interacting nodes. [2] It has battlefield, wildlife spying, fire detection, patient monitoring, intelligent atmospheric, motion monitoring, and flood detection applications [3, 4]. The Key management is a part of security systems in the WSN and it manages cryptographic keys where KMS deals with the generation, storage, distribution, refresh and deletion of key. The KMS provides safe communication among the interacting sensor nodes in the WSN [5].

The sensor nodes in WSN are subjected to various attacks, namely warm hole, tampering, black hole and jamming [6] due to improper security protocols. So, accurate classification of network attacks is important for effective and efficient network security protocols [7, 8]. The unavailability of a key between the end nodes in a sensor network leads to the establishment of the path key scheme [9]. When the source (S) sends a path key to destination (D) through intermediate nodes, the decryption and encryption operations take place on the intermediate nodes. This result increased energy and memory consumption, increased delay in connection or path setup, and the path key is exposed on all these intermediate nodes. The path key comprised of any intermediate nodes and is defined as path key exposure problem [10]. The goals of the path key scheme are given as follows:

1. Reliability: This indicates attackers would not impede D from calculating the path key provided by S. The paths employed to communicate the keys must be reliable.

2. Privacy: The attackers will access the huge number of nodes, so they cannot calculate the path key.

3. Node Capture Resistance: Having captured a significant number of nodes in the network, the attackers may recover the path key [11].

The aforementioned goals are achieved by 3 schemes of proposed path key establishment. The main goals of the proposed model are as follows:

1. An effective model has been developed based on attacker's approach to exploit multiple vulnerable points on the network to destroy the network.
2. This study adopts the adversarial modelling which involves much vulnerability, such as dominant sets, cutting vertices, sensitivity among nodes and paths.
3. In order to enhance the network security, the proposed path key establishment schemes included the attack model of the adversary.
4. The threshold value of k-key fragments is optimized by GWO in PPK scheme.

The organization of this paper is given as follows: Section 2 presents the study of existing works that are related to KMS. Section 3 provides the explanation of the proposed methodology and the experimental results of the proposed methodology are given in Section 4. Finally, the conclusion of this research study is described in Section 5.

2. Literature review

In this section, the study of various existing techniques for key establishment in WSN is presented.

Ahlawa and Dave [12] evaluated the sensor nodes attack coefficient by designing an Attack Matrix (AM) during the position of the sensor in the field. The nodes with high values of attack coefficient were used to minimize the path key exposure. The 3 methods, namely attack-resistant friend-based path key establishment (AFPK), attack-resistant proxy-based path key establishment (APPK) and attack-resistant disjoint path key establishment (ADPK) was developed. The developed method showed improved performance in terms of compromise ratio and key recovery probability. However, the threshold values must be optimized for nodes categorization, which was not considered in this study.

Anzani [13] developed a MerGing Hybrid Symmetric design (MGHS) to solve low connectivity. The MGHS combined the symmetric balanced incomplete blocks in the hybrid designs. The connectivity and resilience were highly improved by the MGHS. The simulation results proved that the MGHS achieved secure network coverage with better resilience for large-scale networks. However, the presence of key pre distribution weakness results into low resilience against denial of service, sinkhole and Sybil attacks.

Zhang [14] studied the sensor network's security by implementing the hybrid schemes for key management schemes that depends on Pool-based key pre-distribution and Basic Random key pre-distribution (PPBR). The connectivity problem for communication link is solved by introducing the tree-based path key establishing technique. The PPBR scheme solved keying scheme issues, such as network resilience and storage efficiency. The PPBR achieved better performance by means of connectivity. However, some issues with the mobile sensor nodes not addressed in real-time scenarios.

Athmani [15] designed an Efficient Dynamic Authentication and Key Distribution (EDAK) pattern for heterogeneous WSNs. While optimizing the security, the main aim of the EDAK is to provide the single lightweight protocol for authentication. The key distribution procedure based on traditional information for generating dynamic keys does not involve secure channels. The EDAK provided better performance in terms of computing time, storage and complexity of the overall key size. However, a check for data integrity is not suggested.

Albakri [16] implemented a new scheme based on polynomials with potential security functions, which effectively reduced the security risk of sensor-driven attacks and consumed only minimal memory and other computing resources. This scheme ensured that the pair would be shared through any sensor node in the key cluster or among the sensor node and its cluster heads (CH). In addition, the proposal has a potential security function that shows robustness to sensor capture attacks. However, the polynomial-scheme needs to optimize the pairwise keys for the security enhancement.

From the analysis of existing techniques, it might be stated that these techniques are insufficient to check the data integrity and also optimization techniques are required to optimize the key fragments for security enhancement. Therefore, GWO is implemented in the PPK scheme to optimize the threshold values for categorization of nodes and k-key fragments, which is described in the next section.

3. Proposed methodology

In order to maintain the PPK, FPK and DPK proposed method, three system models, namely threat model, factors for key fragment and q-Cardinality are described as follows:

Threat Model: Due to the limited resources available to the attacker, the attackers exploit the crucial part of the network in order to cause maximum damage. The crucial part of the network comprises of backbone nodes, path connecting nodes that connect two different parts of the network, type of application that runs on the nodes to create node path insecurity, and attack.

Key fragment factor (k_f): It describes the division of the path key into numerous key fragments, each of which is assigned to the intermediate path nodes towards the destination D [17]. The key fragments may be an equally sized or unequally sized, based on the number of proxies on the path determined by the source S. If the key size is correctly divided by the required sum of k_f key fragments, then fragments of the same size are obtained. In the proposed method, the optimal values of the key fragments are determined by GWO to enhance the redundancy towards the packet loss.

Q-Cardinality (Q): It describes the keys used to establish the communication link that are in common between the one hop neighbor nodes. It describes the strength of the link relative to the number of common keys and enhances link quality with an increase in the number of keys. However, to compromise the link the adversary requires capturing huge network nodes.

In the network, the most secure nodes are identified by the proposed method of path key establishment schemes, where the secure nodes are used to transmit the path key. The three models, namely PPK with GWO, FPK and DPK are developed in this research and are described in the following subdivisions.

3.1 Proxy-based path key establishment scheme (PPK) with grey wolf optimization

The PPK finds for a secure proxy to place a key among two end nodes depleted with a common key. A proxy host is a host that shares keys with S and D. These protected proxies are designated from a set of secure hosts and are used to transmit the path key. To reduce the risk of the path key (k, m), a threshold is set, the GWO accepts list of k-key fragments and determines the optimal k-key fragments by finding the maximum Q values from the list of k-key fragments. The following sections show the brief description of the GWO:

3.1.1. Optimization of key fragments using grey-wolf optimization

GWO technique is derived from the natural hunting and other decision making abilities of the grey wolves that specifically belongs to the Canidae family. Each member in the group plays a part in the hunting process. The apex predators are ranked as the alpha, beta, delta and remaining subordinates are classified as omega. The alpha wolves are the leader of the group in the top of the grey wolf's hierarchy to take the decision about the prey, hunting and food selection [18]. The GWO takes of the hunting and the leadership of the grey wolves and the following are the steps involved in the optimization of the GWO:

1. Track and chase the prey.
2. Pursue, encircle and annoy the prey.
3. Attack the prey.

GWO solution is divided into the three levels based on the fitness and optimality of the solution. In this study, the fittest solution for the optimizing problem is provided by the maximum Q calculated values. The flowchart of the GWO procedure is presented in Fig. 1.

The beta and delta decision are ranked as the next best two solutions and the remaining solution are considered as omega. The Encircling process is given in Eq. (1).

$$\vec{X}(t+1) = \overrightarrow{X_p}(t) + \vec{A}.\vec{Z} \qquad (1)$$

The value of $\vec{Z}$ is given in the Eq. (2)

$$\vec{Z} = |\vec{C}.\overrightarrow{X_p}(t) - \vec{X}(t)| \qquad (2)$$

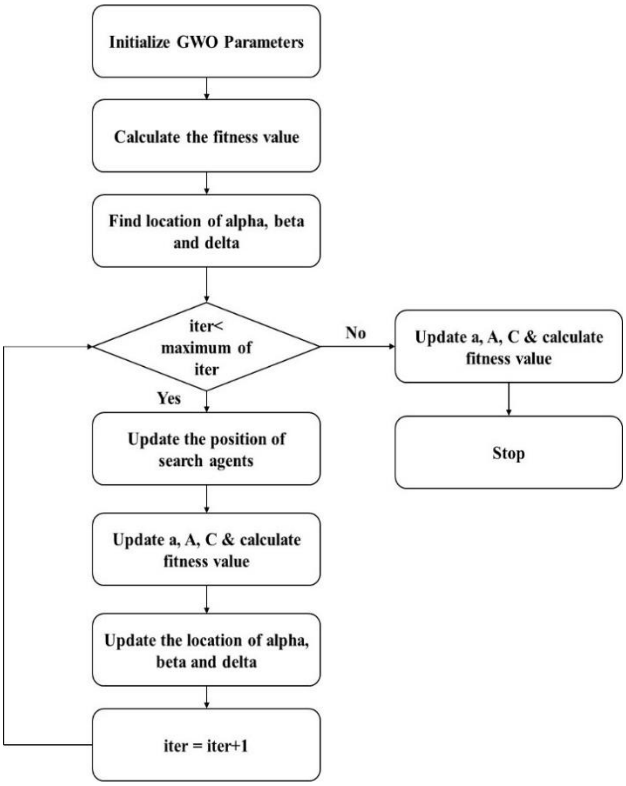
Initialize GWO Parameters
Calculate the fitness value
Find location of alpha, beta and delta
iter< maximum of iter
No
Yes
Update a, A, C & calculate fitness value
Stop
Update the position of search agents
Update a, A, C & calculate fitness value
Update the location of alpha, beta and delta
iter = iter+1

Figure. 1 Flowchart of GWO algorithm

The $\vec{X}$ in the Eq. (1) gives the list of key fragments, $.\overrightarrow{X_p}$ denotes the optimal k-key fragments and t signifies the iteration number, $\vec{A}$ and $\vec{C}$ are the coefficient vector.

The $\vec{A}$ and $\vec{C}$ are manipulated in the Eq. (3) and (4).

$$\vec{A} = 2\vec{A}.\overrightarrow{r_1} - \vec{a} \tag{3}$$

$$\vec{C} = \overrightarrow{2r_2} \tag{4}$$

The components of $\vec{a}$ are lessened from 2 to 0 over the number of iterations, $\overrightarrow{r_1}$ and $\overrightarrow{r_2}$ are the random vector in [0, 1].

Alpha always takes the lead for the searching of the optimal key fragments and alpha, beta and delta know the position of the key-fragments. This process gives the best three solutions to start to update the key-fragments followed by other agents based on the best search agent [19]. The mathematical expression for the position updating is given in the Eq. (5) - (7).

$$\overrightarrow{Z_a} = |\overrightarrow{C_1}.\overrightarrow{X_a} - \vec{X}|, \overrightarrow{Z_\beta} = |\overrightarrow{C_2}.\overrightarrow{X_\beta} - \vec{X}|, \ \overrightarrow{Z_\delta} = |\overrightarrow{C_3}.\overrightarrow{X_\delta} - \vec{X}| \tag{5}$$

$$\overrightarrow{X_1} = |\overrightarrow{X_a} - \overrightarrow{A_1}\overrightarrow{Z_\alpha}|, \overrightarrow{X_2} = |\overrightarrow{X_\beta} - \overrightarrow{A_2}\overrightarrow{Z_\beta}|, \overrightarrow{X_3} = |\overrightarrow{X_\delta} - \overrightarrow{A_3}\overrightarrow{Z_\delta}| \tag{6}$$

$$\vec{X}(t+1) = \frac{\overrightarrow{X_1}+\overrightarrow{X_2}+\overrightarrow{X_3}}{3} \tag{7}$$

The $\vec{X}$ in Eq.(5) denotes the list of key fragments. $\overrightarrow{Z_a}$, $\overrightarrow{Z_\beta}$ and $\overrightarrow{Z_\delta}$ in Eq. (5)-(6) denotes the positions. $\overrightarrow{X_a}$, $\overrightarrow{X_\beta}$, and $\overrightarrow{X_\delta}$ in the Eq. (5)-(6) denotes the best search agent, second best search agent and third best search agent respectively. $\overrightarrow{C_1}$, $\overrightarrow{C_2}$ and $\overrightarrow{C_3}$ is the coefficient vectors. $\overrightarrow{A_1}$, $\overrightarrow{A_2}$, and $\overrightarrow{A_3}$ are also the coefficient vectors.

The pseudo code of GWO is as follows:

Pseudo code for GWO procedure:

```
Initialization of GWO $X_i (i = 1,2, .... n)$ // $n$ is the length of key fragments list, $X$ represents the list of key fragments and $i$ denotes the each key fragments.
Initialization of $\overrightarrow{A}, \vec{C}$ and $\vec{a}$ parameters //list of k-key fragments
 Every agent or wolf fitness value
        $X_\alpha$  best search agent
        $X_\beta$ second  best search agent
        $X_\delta$ third  best search agent
while $t <$ max number of iterations
   for each search agent
     update the station of current search agent
   end for
update $a$, $A$ and $C$
Compute fitness of total search agents// maximum Q calculated value
update $X_\alpha$, $X_\beta$, and $X_\delta$
        $t = t + 1$
end while
return $X_\alpha$// optimal $k_o$ –key fragments
```

In addition, intelligent swarming methods are used to solve an optimization problem, which do not have a leader to monitor the process. This limitation is addressed using the GWO method. The Grey wolves have individual leadership qualities and find the optimal threshold based on minimum fitness value. Therefore, this research uses the GWO to find the optimal k_o- key fragments from the optimal k-key fragments according to maximum Q calculated value. For instance, the GWO uses the population size as 6 capture nodes and number of iterations is 3, the proposed PPK with GWO achieved the 0.265 probability of key recovery. In addition, when the number of nodes is increased to 60, the proposed PPK with GWO achieved 0.035 probability of key recovery, where the existing APPK achieved 0.039

probability of key recovery. The results show that the proposed PPK achieved better performance using the optimal k-key fragments.

The PPK with GWO procedure is as follows:

- The path keys are set by Source ‘S’ and Destination ‘D’ nodes.
- The list of key identifiers is forwarded by node S to the node D.
- Node D produces a path key that is unique between a pair of nodes S and D for communication and splits the key into diverse fragments of keys as mentioned by a key fractional coefficient, so $K = K_1 \cup K_2 \cup K_3 \dots K_k$.
- This final threshold K_k is optimized using GWO. Each key fragment is numbered and the last fragment is provided with a CRC to ascertain the correctness of the fragment.
- The Destination D identifies optimum ‘K’ number of proxy nodes from a set of secure nodes with the maximum number of Q elements using GWO.
- After obtaining all the key fragments, Node S restores the original key and checks for the integrity. The next sub-section presents the proposed FPK procedure.

3.2 Friend-based path key establishment scheme (FPK)

The selected nodes of this scheme share a common key with D that is identified as secure nodes. Algorithm 1 represents the selection process of secure friend nodes.

Algorithm 1: To identify the secure friend nodes in the network

```
Code at Source node:
Input: Destination node $d$
Output: Path Key $K_{sd}$ transferred with friend nodes
Set the value of $TTL = h$
Receive part-keys from trusted nodes in the reply of the request for path key set up with $d$
Select the part keys of $i$ with minimum and maximum of q-cardinality;
Let $pk_e$ be encrypted key fragments with HEB=1 and $i - pk_e$ are unencrypted key fragments with HEB=0;
for $j = 1$ to $pk_e$ do
    $pk_j = E_d$ (Selected part-key $j$, $KST_j$)
end for
for $j = ne + 1\ to\ i$ do
    $pk_j =$ Selected part-key $j$
end for
$K_{sd} = g(pk_1, pk_2, \dots, pk_i)$
return $K_{sd}$
Code at $T_j$ (Transmitting node of $j$):
Input: Destination node $d$
Output: $pk_T, q_{T-d/s}pk_T = 0; F_d = 0; HEB = 0; flags = 0;$
for $m = 1\ to\ k$ do
    for $l = 1\ to\ k$ do
        if ($KT_m == KD_l$) then
            $pk_T = XOR(pk_T, truncated\ KT_m)$
            $F_d = 1$
        end if
    end for
end for
if ($F_s == 1$) $and$ ($F_d == 1$) then
    $pk_T = E_d(pk_T, KST)$
    HEB=1
end if
if ($pk_T = null$) then
    Send $pk_T$ and identify $T$ to $S$
else if (TTL_=0) then
    Broadcast request packet to neighbors
Else
    drop the packet
end if
Return $K_{sd}$
```

Algorithm 1 works as follows: Safe nodes are the one which is selected as friend nodes and source node asks those nodes for path key establishment. The neighbor that shares a key with the D and in return D responds with partial keys before the expiry of TTL. These keys are encrypted or forwarded in the plain text to D, subject to the shared keys that are available to the friend nodes. The key produced by Source encrypted and is forwarded to D. Once the path key is received, then the destination node decrypts and new path key is obtained.

3.3 Disjoint path key establishment scheme (DPK)

The DPK scheme takes node Q-cardinality and the length of the path to choose the best path. In this arrangement, k optimized key fragments are transmitted along the disjoint paths towards the destination, and are combined to construct a path key. Further, an increase in the disjoint path not only increases the intermediate nodes, but also magnifies the key exposure problem. The length of the path takes into account the number of intermediate nodes enroute to D. Let the probability of node compromise bep_i, then the possibility of compromising the

l −hops path (p_c) is given in the following Eq. (8);

$$p_c = 1 - (1 - p_1)(1 - p_2) \dots (1 - p_l) \qquad (8)$$

This indicates that longer routes are compromised easily than shorter routes, so the shortest path must be the preferred path.

3.3.1. Working of the DPK Scheme

The suggested DPK scheme has two stages: a data collection and multiple disjoint route detection stage. The first step enables the source to use a path-based routing algorithms to explore routes and gather information regarding the Q of the participating nodes. The second stage decides the best path for the path key establishment by analysing the first stage information along with the path length. The algorithm 2 describes the process of DPK.

Algorithm 2: To discover the disjoint path for key establishment

```
Input: S, D, $k$ (optimal-key fragment factor), $PL_{threshold}$;
Output: $P_{selected}$;
Compute the node disjoint paths $p_1, p_2, p_3 \dots p_k$ for given $< s, d >$ pairs;
Set $P_{discarded} = 0$;
for $i = 1\ to\ k$ do
if $\exists x \in P_i \&\& PL_x^t \leq PL_{threshold}$ then
Discard $P_i$
$P_{discarded}$=$P_{discarded} + 1$
end if
end for
if $N_{discarded} = k - 1$, then
$P_{selected}$=P
exit
end if
$N_{discarded} = kthen$
$P_{selected} = P_i\ with\ \min\_PL_X^t$
exit
end if
$\forall x \epsilon P_i\ compute\ FAC_X^i = \frac{1}{AC_X^t}$, where $l \leq i \leq k \&\& x \notin S, D$
Compute $AV[P_i] = \sum_{x \in P_i} FAC_X^i + q_X^i$; where $x \notin S, D$
MAX=AV[P1]
for $i = 2\ to\ k$ do
if $AV[P_i] > MAX$ then
$AV[P_i] = MAX$
$M = i$
end if
end for
select and return the path $P_{selected} = P_M$
```

Algorithm 2 works as follows: DPK starts by finding several split paths from source node S destination node D within the sensor network. Thus, the shortest length path with minimal attack coefficient along with highest Q-values is selected to forward the fragments of the key to D. Thus the proposed scheme offers a secured path for communications.

4. Results and discussion

The performance of the three proposed models is analysed in this section. The C++ programming is used for the simulation setup with a network size of 50 nodes.

4.1 Performance of PPK-with grey wolf:

Resilience and over node capture is considered to assess the performance of the PPK with GWO algorithm, where resilience is described as the possibility of extraction of minimum of K fragments by capturing as many as X nodes. The newly created path key is encrypted with the proxy node keys. In order to intercept the fragments of the path key sent through the proxy, the attacker must identify the encryption key used in this proxy node. Therefore, the probability P_R that one out of 2m keys available in a node is t/p, where t is the size of the ring and P is the size of the pool. The likelihood of k key distributed sized nodes presented in the key-sets of the proxy nodes shown in the Eq. (9):

$$P_R = \sum_{l=k}^{m} 1 - ((1 - \frac{(L+1).t}{2L.P})^x)^{2l} \qquad (9)$$

This probability does not be contingent on the sum of network nodes. The proxy K uses least key pairs which are less than m pairs to protect the m-key fragments, then the redundancy of the PPK will be increased.

Resilience over the capture of a node can also be the ability of an attacker to extract fragments of the key pair and the keys are completely compromised if either the source S or destination D is in the captured nodes, whose probability p_1 as described in Eq. (10):

$$p_1 = \frac{\left(\frac{2n-x-1}{x-1}\right).\binom{n-2}{x-2}}{\binom{n}{x}} \qquad (10)$$

The source or destination isn't in the captured node group and the captured group has at least k-proxies are given by probability p_2 is defined in the Eq. (11):

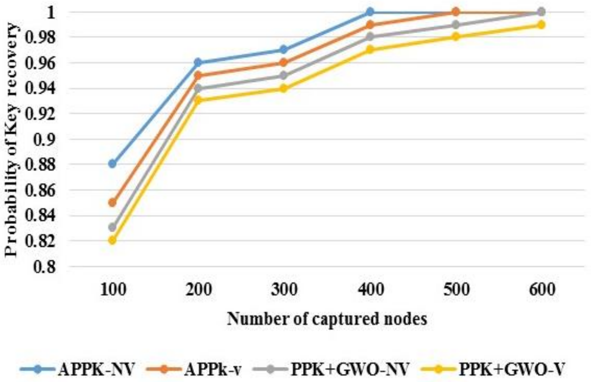

Figure. 2 Comparative analysis of proposed PPK-with Grey wolf with other APPK

$$p_2 = (1 - P'').\sum_{l=k}^{m} \frac{\binom{m}{l}.\binom{n-m-2}{x-l}}{\binom{n}{x}} \qquad (11)$$

Where, P'' is connectivity key. Further, all the shared keys are exposed to an adversary and are defined in the Eq. (12)

$$p_f = p_1 + p_2 \qquad (12)$$

Further p_f is defined in the following Eq. (13) as:

$$p_f = \frac{\left(\frac{2n-x-1}{x-1}\right).\binom{n-2}{x-2}}{\binom{n}{x}}.(1 - P''). \qquad (13)$$

The number of compromised and distributed nodes in the network as presented in the Eq. (13) decides the probability of the safe nodes revealing the path key, as m proxies are only selected from safe node set. Therefore, compromising a node from vulnerability set does not affect the probability.

P'_{k-p} the likelihood that existence of p proxies and their presence in x captured network nodes. P_{k-p} is defined in the Eq. (14)

$$P'_{k-p} = \sum_{l=k}^{m} \frac{\binom{m}{l}.\binom{n-m-2}{x-l}}{\binom{n}{x}} \qquad (14)$$

An increase in proxy servers from 3 to 5 results in a significant increase in the GWO-PPK scheme's security.

Fig. 2 shows the PPK scheme with GWO and APPK [12] in terms of probability of a significant recovery. The PPK+GWO-V and PPK+GWO-NV are used, GWO-NV with PPK is a presumption that only legitimate nodes exist in the network. As the number of nodes increases the probability of key recovery is distributed. The GWO-V with PPK is a variation presuming the existence of negligible number of weak nodes in the network.

When compared with APPK-V [12] and APPK-NV [12], the proposed GWO with PPK has lower key recovery probability because of the distribution of the hash chain in a manner that avoids the potential unsafe nodes during the path key setup phase. The R = 40, L = 10, P = 1000, K = 6, are considered and the scheme is not immune. If the attacker is capable of compromising the significant number of nodes, then the probability of nodes in the network being compromised and attains unity as much of the key pool gets exposed. In existing APPK [12] and APPK-NV [12] k- key fragments are taken as number of safe proxies found by Destination D. The proposed PPK+GWO-V and PPK+GWO-NV shows higher performance due to the optimal k_o −key fragments obtained from the actual k-key fragments and categorization of sensor nodes.

4.2 Performance of proposed FPK:

The D and S are not comprised and an attempt is made to study the similar key recovery by capturing the secure nodes. Let n denote the proxy nodes used in the path key generation by S and X denoted the seized nodes. Further, it needs to be understood that compromising the insecure node does not necessarily expose the path key as these nodes are not considered in the selection of the path key. Hence this considers the safe nodes for the purpose of security analysis.

Let E denote the presence of a n number of proxies in the x, E^c be the event where the attacker is unable to extract the secret key, m be the number of network nodes without considering S, D the total safe nodes in the list x be denoted by r. Let A_L be the event attacker extracts the path key in an L number of attempts. Therefore $P(A_L)$ can be determined using the Eq. (15).

$$P(A_L) = P(E^c)P(A_L E^c) + P(E)(P(A_L|E) \qquad (15)$$

The value of $P(E^c)P(A_L|E^c)$ is zero and in order to calculate $P(A_L)$, $P(E)$ and $\big(P(A_L|E)\big)$ are essential and is shown Eq. (16).

$$\text{Where } P(E) = \frac{\binom{m-n}{x-n}}{\binom{m}{x}} \qquad (16)$$

The $P(A_L|E)$ is computed in Eq. (17)

$$\sum_{f=n}^{x} P(A_L, Z = f|E)$$
$$\sum_{f=n}^{x} P(A_L|Z = f, |E)P(Z = f|E) \qquad (17)$$

Considering the F friends / proxies available, then the probability that appropriate grouping of proxies

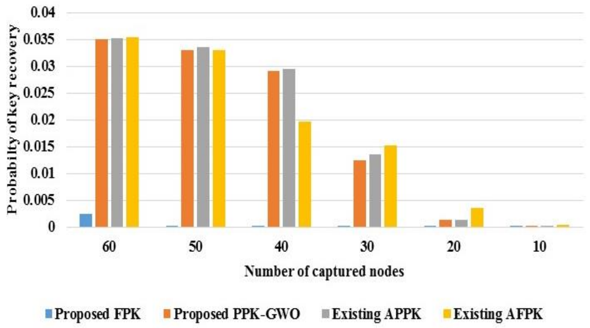

Figure. 3 Comparative examination of diverse scheme on the possibility of key recovery for dissimilar values of $i = 10$

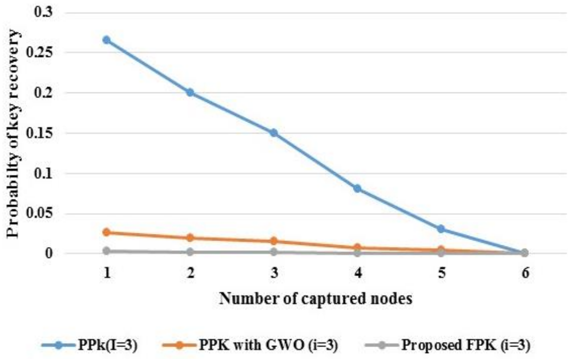

Figure. 4 Comparative examination of diverse arrangement on the possibility of key recovery for diverse values of i=3

by attacker in the first attempt is $\frac{1}{\binom{f}{n}}$ and the complete likehood of the same is expressed in Eq. (18)

$$\sum_{k=i}^{x} \frac{\min L, \binom{k}{i}}{\binom{k}{i}} \tag{18}$$

Using the binomial distribution, $P(z = f|E)$ in Eq. (19),

$$\binom{x-n}{f-n} p^{k-i}(1-p)^{x-k} \tag{19}$$

Where, p is the probability of a node being a friend. By using the aforementioned Equations, the probability of attacker extracting the key P_{kr} within L runs is determined using the Eq. (20).

$$P_{kr} = \frac{\binom{m-n}{x-n}}{\binom{m}{x}} \sum_{f-n}^{x} \frac{\min L, \binom{f}{n}}{\binom{f}{n}} \binom{x-n}{f-n} p^{f-n}(1-p)^{x-f} \tag{20}$$

A comparative plot of the PPK, PPK with GWO and FPK for various ‘i’ values is presented in Fig. 4. When the number of nodes are less the probability of key recovery decreases. The results show that the probability of the key compromises with FPK is fewer than with PPK and Fig. 3 illustrates key recovery probability for various methods. The graph considers m = 60, q = 0.216, p = 0.466 and L = 100. The obtained results present good resilience against nodes capture, as susceptible nodes are ignored and only safe nodes are preferred as a part of the friend node selection process. The proposed FPK shows higher performance due to the optimal key fragments and categorization of sensor nodes.

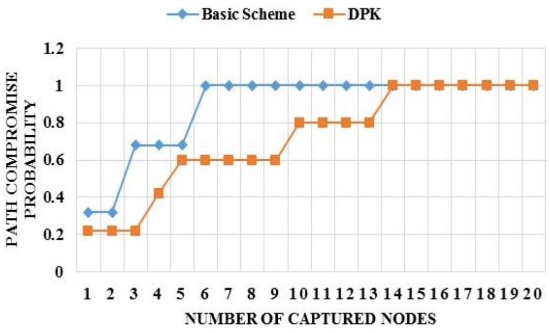

Figure. 5 Comparative examinations of DPK with basic arrangement for path compromise ratio for 20 nodes

PPK with GWO due to increased key fragments and offer better immunity against node capture. However, the scheme suffers from increased communication cost.

4.3 Performance of proposed DPK

The proposed DPK method allows the path key to be sent over any given S and D pair through a series of highly secure disjoint routes. The minimum length route discovery is implemented with the help of a route selection constraint being the minimum attack coefficient and a maximum Q value. The performance is evaluated by the route compromise ratio and is defined as the ratio of compromised routes to the total routes available on the network between the source and the destination node.

Fig. 5 shows the proposed DPK has the lowest path compromised values, as a result of maximum value of Q and the lowest attack coefficient value (ADPK [12]). When the number of nodes and key fragments are equal that time probability will not get distributed. It is observed that the scheme offers an improved resilience against enroute path nodes which are less likely to be captured.

The analysis of the impact of the variations in the size of the key and the size of the path key fragments is drawn upon the computational costs associated with the path key decomposition process. The size of the ending fragment and the first key fragments

Table 1. Function of key length

Number of Key fragments	k(s) 128 bit		k (s) 64 bit	
	First fragment size	Last fragment size	First fragment size	Last fragment size
k=1	65	65	32	32
k=2	43	45	20	24

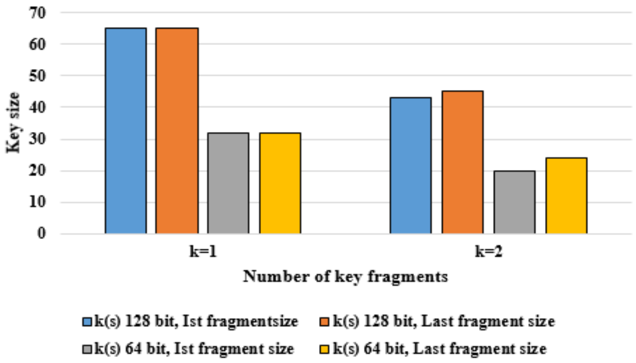

Figure. 6 Variation of the dimension of first and last fragment as a function of key length

changes along with the size of the key and the total number of fragmentations of a particular path key. The proposed DPK shows higher performance due to the optimal key fragments and categorization of sensor nodes. From the analysis of existing techniques [12], it might be stated that these techniques are insufficient to check the data integrity and also optimization techniques are required to optimize the key fragments for security enhancement. Therefore, GWO is implemented in the PPK scheme to optimize the threshold values for categorization of nodes and k-key fragments.

The fragments will be of same size when the key size is divided by the total number of key fragments. The ending fragments will have a varied fragment size as shown in Fig. 6. Table 1 shows the results for different key fragment sizes.

5. Conclusion

WSN is the most imperative infrastructures for new remote networked communications and is vulnerable to various attacks. To minimize the impact of path key exposures on sensor nodes, three path-based schemes are presented in this study, namely PPK, FPK, and DPK. The threshold value of the node categorization and k-key fragment is optimized using the GWO algorithm in the PPK system. The experimental results of the PPK scheme with GWO have at least significant key recovery probability with the elementary APPK and AFPK schemes. FPK has the best security features with varied values of$i$. The proposed PPK-GWO achieved the probability of key recovery is 0.8 for 100 captured nodes, The DPK achieved the probability of path compromise is 0.95 for 10 captured nodes. The proposed DPK minimised the path compromise and effects of node capture. In the future work, the researchers plan to develop a hybrid optimization for dynamic authentication techniques and KMS in heterogeneous WSN.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 1st author. The paper conceptualization, methodology, software, validation, formal analysis have been done by 3rd author. The supervision and project administration, have been done by 2nd author.

References

[1] M. S. Yousefpoor and H. Barati, “Dynamic key management algorithms in wireless sensor networks: A survey”, *Computer Communications*, Vol. 134, pp. 52-69, 2019.

[2] F. Gandino, C. Celozzi, and M. Rebaudengo, “A key management scheme for mobile wireless sensor networks”, *Applied Sciences*, Vol. 7, No. 5, pp. 490, 2017.

[3] P. Ahlawat and M. Dave, “An attack model based highly secure key management scheme for wireless sensor networks”, *Procedia Computer Science*, Vol. 125, pp. 201-207, 2018.

[4] J. Zhang, H. Li, and J. Li, “Key establishment scheme for wireless sensor networks based on polynomial and random key predistribution scheme”, *Ad Hoc Networks*, Vol. 71, pp. 68-77, 2018.

[5] A. G. Dinker and V. Sharma, “Trivariate polynomial based key management scheme (TPB-KMS) in hierarchical wireless sensor networks”, *Ambient Communications and Computer Systems*, pp. 283-290, 2018.

[6] K. Venkatraman, J. V. Daniel, and J. Murugaboopathi, “Various attacks in wireless sensor network: Survey”, *International Journal of Soft Computing and Engineering (IJSCE)*, Vol. 3, No. 1, pp. 208-212, 2013.

[7] N. Athavale, S. Deshpande, V. Chaudhary, J. Chavan, and S. S. Barde, “Framework for threat analysis and attack modelling of network security protocols”, *International Journal of Synthetic Emotions (IJSE)*, Vol. 8, No. 2, pp. 62-75, 2017.

[8] K. Moara-Nkwe, Q. Shi, G. M. Lee, M. H. Eiza, "A novel physical layer secure key generation and refreshment scheme for wireless sensor networks", *IEEE Access,* Vol. 6, pp. 11374-11387, 2018.

[9] W. Bechkit, Y. Challal, A. Bouabdallah, and V. Tarokh, "A highly scalable key pre-distribution scheme for wireless sensor networks", *IEEE Transactions on Wireless Communications*, Vol. 12, No. 2, pp. 948-959, 2013.

[10] M. Jamshidi, H. Bazargan, A. A. Shaltooki, and A. M. Darwesh, "A hybrid key pre-distribution scheme for securing communications in wireless sensor networks", *JOIV: International Journal on Informatics Visualization*, Vol. 3, No. 1, pp. 41-46, 2019.

[11] S. H. Jokhio, I. A. Jokhio, and A. H. Kemp, "Node capture attack detection and defence inwireless sensor networks", *IET Wireless Sensor Systems*, Vol. 2, No. 3, pp. 161-169, 2012.

[12] P. Ahlawat and M. Dave, "Secure Path Key Establishment Schemes Based on Random Key Management for WSN", In: *Proc. of the National Academy of Sciences, India Section A: Physical Sciences*, pp. 1-13, 2020.

[13] M. Anzani, H. H. S. Javadi, and V. Modirir, "Key-management scheme for wireless sensor networks based on merging blocks of symmetric design", *Wireless Networks,* Vol. 24, No. 8, pp .2867-2879, 2018.

[14] Y. Zhang, J. Liang, B. Zheng, and W. Chen, "A hybrid key management scheme for WSNs based on PPBR and a tree-based path key establishment method", *Sensors*, Vol. 16, No. 4, pp. 509, 2016.

[15] S. Athmani, A. Bilami, and D. E. Boubiche, "EDAK: An efficient dynamic authentication and key management mechanism for heterogeneous WSNs", *Future Generation Computer Systems*, Vol. 92, pp. 789-799, 2019.

[16] A. Albakri, L. Harn, and S. Song, "Hierarchical key management scheme with probabilistic security in a wireless sensor network (WSN)", *Security and communication networks*, 2019.

[17] A. Ghafoor, M. Sher, M. Imran, and A. Derhab, "Secure key distribution using fragmentation and assimilation in wireless sensor and actor networks", *International Journal of Distributed Sensor Networks*, Vol. 11, No. 9, pp. 542856, 2015.

[18] S. Mirjalili, S. M. Mirjalili, and A. Lewis, "Grey wolf optimizer", *Advances in Engineering Software*, Vol. 69, pp. 46-61.

[19] S. Mirjalili, S. Saremi, S. M. Mirjalili, and L. D. S. Coelho, "Multi-objective grey wolf optimizer: a novel algorithm for multi-criterion optimization", *Expert Systems with Applications*, Vol. 47, pp. 106-119, 2016.