OPTIMAL CLUSTER BASED KEY MANAGEMENT SYSTEM USING SIGNCRYPTION ALGORITHM FOR WIRELESS SENSOR NETWORKS

G. Manikandan[*], *U. Sakthi*[†]

Abstract: Key management system maintains the confident of secret information from unauthorized users and verifying the integrity of exchanged messages and authenticity. But recent advances in electronics and computer technologies create the complexity of key management in wireless sensor networks (WSN). Additionally, the traditional key management systems are not up to the mark due to limited resources like memory, and energy constraints.In this paper, we propose an optimal cluster based key management system (OC-KMS) for WSNs. The proposed system consist of two contributions, in first, we perform the energy efficient clustering using modified animal Diaspora (MAD)optimization algorithm and cluster head (CH) selection using JAYA trust model. In second contribution, we propose the certificate less signcryption algorithm, which generates and distributes the public and private keys for each node in sensor networks. The proposed system resists various network layer attacks without affecting the network performance. The simulation resultdescribes that the proposed system perform very efficient than existing in terms of both performance and security wise.

Key words: *clustering, cluster head, Modified Animal Diaspora (MAD) optimization, JAYA trust model, signcryption*

Received: July 17, 2017 **DOI:** 10.14311/NNW.2018.28.024
Revised and accepted: July 20, 2018

1. Introduction

WSN is a network formed by a large number of sensor nodes, each equipped with sensor to detect physical phenomena such as heat, light, motion, or sound [1]. Utilizing specific sensors, WSNs can be executed to fortify different applications including security, distraction, mechanization, mechanical watching, open utilities, and resource association [2]. Regardless, different WSN gadgets have exceptional asset targets to the degree centrality, estimation, and memory, acknowledged by a

[*]G. Manikandan – Corresponding author; Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Tamilnadu, India, E-mail: gmanikandan2516@gmail.com

[†]U. Sakthi; Department of Computer Science and Engineering, St. Joseph's Institute of Technology, Chennai-119, India, E-mail: sakthi.ulaganathan@gmail.com

need to restrict the cost of the gigantic number of gadgets required for a couple of uses and by sending conditions that check direct access to the contraptions. Before trade information safely, encryption keys must be created among sensor focus focuses [3]. Key dispersing proposes the diffusing of different keys among the sensor focuses, which is regular in a non-superfluous security plot [38]– [40]. Key association is a more wide term for key task, which in like way breakers the system of key setup, the basic spread of keys, and key revocation the clearing of a wrangled key [4]. Despite the way that considers key use for secure information transmission, it doesn't choose how to trade keys safely. This leaves open the key association issue that is the centralization of much late research [5]. Other than the affiliation layer, upper layers, for example, the structure and application layers in like way should trade keys safely [6]. Different security-fundamental applications rely on upon key association philosophy to work likewise request an abnormal state of acclimation to inside disillusionment when a middle point is traded off [7]. This is a basic issue in light of the way that there are different stringent prerequisites for key association, and the advantages open to execute such system are uncommonly compelled [8]. A classical random key management and distribution scheme for WSNs are Eschenauer, Du, LEAP, SHELL, and Panja [41].

Eschenauer et al. [9] have designed to satisfy both operational and security requirements of DSNs. The scheme includes selective distribution and revocation of keys to nodes as well as node rekeying without substantial computation and communication capabilities. Another key pre-distribution scheme [10], which substantially improves the resilience of the network compared to the existing schemes. Localized encryption and authentication protocol (LEAP) [11] for sensor networks have designed to support in-network processing, while at the same time restricting the security impact of a node compromise to the immediate network neighborhood of the compromised node. Exclusion basis systems (EBS) based distributed key management scheme, named as SHELL [12], and implemented by combinatorial formulation for the group key management problem. It supports rekeying and enhanced framework security and survivability against center catch. It uses a key assignment plot that decreases the capacity of interest among dealt sensor nodes by figuring the geographic territory of centers in key errand [42]. A group key management protocol [13] for hierarchical sensor networks have developed from pre-deployed keys, each sensor node generates a partial key dynamically using a function. The function takes partial keys of its children as arguments.

A dynamic key management scheme based on localized combinatorial keying (LOCK) [14] have been proposed for sensor networks that are dynamically establish, maintain secure channels among sensor nodes. Combinatorial design based deterministic and hybrid approach assign keys to each key-chain before the sensor network deployment. Balanced incomplete block designs (BIBD) and generalized quadrangles (GQ) mapped to obtain efficient key distribution schemes [15]. Unified frameworks for distributed key management scheme [16] for heterogeneous wireless sensor networks have developed to evaluate the performance in terms of connectivity, reliability, and resilience. Deployment knowledge based key management scheme [17] with a target field divided into hexagon grids and sensor nodes are divided into the same number of groups as that of grids, where each group deployed into a unique grid [43].

A simple and practical location-based pair-wise key pre-distribution scheme [18] achieves higher connectivity and perfect resilience with much less consumption of resources. A routing-driven key management scheme [19] has establishes shared keys for neighbor sensors that communicate with each other using elliptic curve cryptography (ECC). This scheme provides better security with significant reductions on communication overhead, storage space and energy consumption than other key management schemes.Constrained random perturbation-based pair wise key establishments (CARPY) scheme [20] have satisfied requirements in sensor-key criteria's are resilience to the adversary's intervention, directed and guaranteed key establishment, resilience to network configurations, efficiency, and resilience to dynamic node deployment. ECC and signcryption method based dynamic key management scheme [21] have network scalability and sensor node (SN) mobility especially in liquid environments. The periodic authentication and registration mechanism have used through prevention of SN compromise. Alternatively, the frequency selectivity of multipath fading channels based key generation protocols [22] have not required device movement during key establishment. Enhanced unital-based key pre-distribution scheme [23] providing high network scalability and good key sharing probability approximately lower bounded. An intra-cluster key sharing (IKS) scheme combined with low-energy key management (LEKM) protocol [24] for increasing the resilience against node capture during network initialization.

Contributions In this paper, we propose an optimal cluster based key management system for WSNs (OC-KMS). The proposed system performs the cluster formation using modified animal Diaspora (MAD) algorithm and JAYA trust model. Then certificate less signcryption algorithm used to encrypt the forwarded information's in each source node.

The remaining paper is organized as follows: Section 2 discuss the recent works related to our contributions. In Section 3, the problem methodology and system model of proposed key management system are introduced. The detailed description of proposed key management system is present in Section 4. In Section 5, experiments and evaluations are conductedto the proposed system. Finally, the paper is concluded in Section 6.

2. Related works

Seo et al. [25] have proposed a certificate less effective key management protocol (CL-EKM) for dynamic WSNs characterized by node mobility. CL-EKM supports gainful key updates when a center point leaves or joins a gathering and certifications forward and in turn around key. The tradition furthermore supports beneficial key repudiation for bartered centers and constrains the impact of a center point exchange off on the security of other correspondence joins. This scheme was resilient against node compromise, cloning and impersonation attacks and protects the data confidentiality and integrity. However, CL-EKM is not fitted to high density sensors with high resources and unable to perform expensive computations with huge key sizes.

Gandino et al. [26] have presented an innovative key management scheme, named as random seed distribution with transitory master key, which adopts the random distribution of secret material and a transitory master key used to generate pair wise keys. This approach addresses the main drawbacks of the previous approaches based on these techniques. However, it is not able to compromise resilient against cluster head capture, as a result of the cluster head at random generates a pair-wise key between sensing element nodes whenever it's requested by the nodes.

Lalitha et al. [27] have proposed presented a mobility management technique for keying scheme of WSNs. The technique selects nodes with high essentialness resources, wide correspondence range and high taking care of cutoff as CH. Gather keys for CH and consolidate smart keys for centers are made by the sink through dismissal introduce structures. At whatever nodes moves from at present related group to another in the network, the compactness based key organization plan was actuated. The sink checks the validness of meandering center point and doles out it to a near to bundle. The common thread of this technique is the fact that the applications face limitations imposed by WSNs. The limitations stem from the short life time, limited computation capabilities, large number of nodes deployed, lack of infrastructure, besides the possible mobility nature of sensory devices causing frequent topology changes.

Anita et al. [28] have proposed Q-composite key generation scheme with the polynomial pool-based scheme that enables a secure communication between wireless sensor nodes. The security analysis assures a high probability of secure communication with a low communication overhead. This scheme inherits the strength of Q-composite and polynomial schemes leading to the triple key establishment between any three nodes. This scheme performs better in terms of network resilience against node capture attacks with a high probability of connectivity and improves the compromised data links between non compromised sensors.

Messai et al. [29] have proposed sequence-based key management (SKM) for WSNs. The sensor nodes focuses are pre-scattered with the fundamental term and the recursive equation of a numerical social event. This two little pre-scattered data's have guarantee the foundation of merge smart keys to every sensor node with its neighbors after sending with a little measure of figuring. The SKM techniques ability and lightweight in term of focus focuses assets and has a decent versatility against focus point wheeling and dealing ambushes.

Sun et al. [30] have proposed self-healing key management schemes based on modified access polynomial and it was broadcast authentication and enhanced collusion resistance. Two different attacks have introduced to break the security of access polynomials. A modified security model, collusion resistance capability was redefined from the perspective of session interval from node revocation to node addition, which does not depend on the number of collusive nodes.

Kumari et al. [31] have investigated the commutatively under composition and semi-group property of extended Chebyshev polynomials and proposed a secure key management scheme. The scheme for WSN creates session key among client and sensor focuses utilizing augmented wild maps by control of which the created session key gives the forward mystery. This scheme provides user secret and mindful of stolen-verifier assaults. The communication overhead of this scheme was adequately less but affected by memory issues when emerged from past schemes.

Gandino et al. [32] have presented the hierarchical key management scheme using transitory master key (HSTMK).This scheme was proposed for static WSNs with focus nodes including property and without sending learning. HSTMK lessens the time window in which an enemy can complete key confuse material from the memory of the inside purposes of the system. A gainful relationship of the handshake routine was subdivided into discrete stages and it lessens the measure of groups traded amidst each stage. The lower number of packs makes a diminishment in the measure of impacts and permits a shorter key setup time.

Zhan et al. [33] have handled the problem of key connectivity and proposed system of equation based key generation method, which improves the key connectivity of key management. The included equations have related with create mystery keys and each inside point utilizes these keys for securing their correspondence. The neighbors can obviously converse with each other through customary canvassed enter notwithstanding the way that they utilize related keys.

Anzani et al. [34] have proposed a hybrid key pre-distribution approach based on the symmetric combinatorial based design. They merge the squares of symmetric course of action to make new key-rings as opposed to making contrasting plot, which was gotten a handle on in cross breed symmetric approach, named as merging hybrid symmetric design (MGHS). It makes a test set in a more productive manner and acquaints a parameter with pick the measure of combined pieces to convey key-rings. This approach enhances the arrangement of cream symmetric course of action and not gives better flexibility against focus point get assault.

3. Problem methodology and network model

3.1 Problem methodology

Zhang et al. [35] have presented a dynamic key management method (DKMM) for WSNs. The method considers the discover probability as network clustering, and the nodes which hold cut down catch probability the CH first. The key organization procedure has achieved the dynamic key update and deals with the issue of structure security resistance when the gathering heads are gotten. This key organization framework makes more secure nodes no doubt have the chance to twist up clearly the CHs. Notwithstanding the way that considering the prosperity of the CHs while gathering, the CHs may even now be possible to be gotten. So DKMM procedure considers how conceivable it is that the CH may be gotten. The affirmation of CHs reselection parts and the dynamical invigorating instruments of the keys are main risk of information spilling due to the CHs get. DKMM provides anti-destroying ability (higher security) than other methods in terms of multiple nodes are captured within a cluster at the same time; this will not reveal the keys between other nodes. But DKMM will not suitable for recent networks attacks like block hole (BH), worm hole (WH), gray hole (GH), rushing attack, and key-compromising attack [36]. DKMM loss the impress on clustering process, because not aware of sensor node movement (special case, it is possible) and CH node lifetime. Additionally, they consume more energy for CHs reselection process.

For that reason, our proposed OC-KMS key management systemneeded must to overcome those problems by optimal clustering manner with effective key man-

agement in terms of new node enter/leave in/from the cluster. First, the energy efficient clustering techniques performed by modified animal Diaspora (MAD) optimization algorithm and JAYA trust model. The MAD algorithm inspired from the conventional animal migration optimization (AMO) algorithm [37]. Here, we use MAD algorithm for cluster formation and select CH among cluster members using trust inference model called JAYA trust model. The combined optimization and trust model provides better clustering than particle swarm optimization (PSO) in DKMM method [35]. Second, generates and distributes the public, private keys for each node and perform encryption usingcertificate less signcryption algorithm. Main contributions of proposed system as follows:

1. Proposed OC-KMS consist of two contributions such as optimal-trust clustering and effective key management, which provides double security in terms of trusted path and encrypted data with key management system.

2. The proposed clustering technique aware of node enter/leave in/from every cluster in the network, then base station selects the CH based on highest trust value. The trust values of each node are calculated by different node constraints are energy consumption, received signal strength, and mobility.

3. Certificate-less signcryption achieves confidentiality and authentication by combining public-key encryption and digital signatures, which provides better performance and aware of network layer attacks.

3.2 Network model

The network model for our proposed work is shown in Fig. 1. The network consists of base station (BS), sensor node members, and cluster head nodes (CHs). BS employed to gather the information from sensor nodes, and compute trust value. Based on the trust values BS select the CH for every cluster, which collect all the information from other nodes in own cluster. The CHs are only eligible to directly communicate with the neighboring CHs node and the BS. The each node in the cluster has a unique ID and is randomly deployed.For data transmission between source to destination node performed by certificate-less signcryption algorithm.

4. Optimal cluster based key management system (OC-KMS)

This section first discusses the clustering techniques in Subsection 4.1 and the key management system present in Subsection 4.2.

4.1 Clustering technique

4.1.1 Cluster formation using modified animal Diaspora (MAD) optimization algorithm

The movement is tenacious and changed change influenced by the creature's own particular locomotors attempts passing on them to new typical condition. It relies

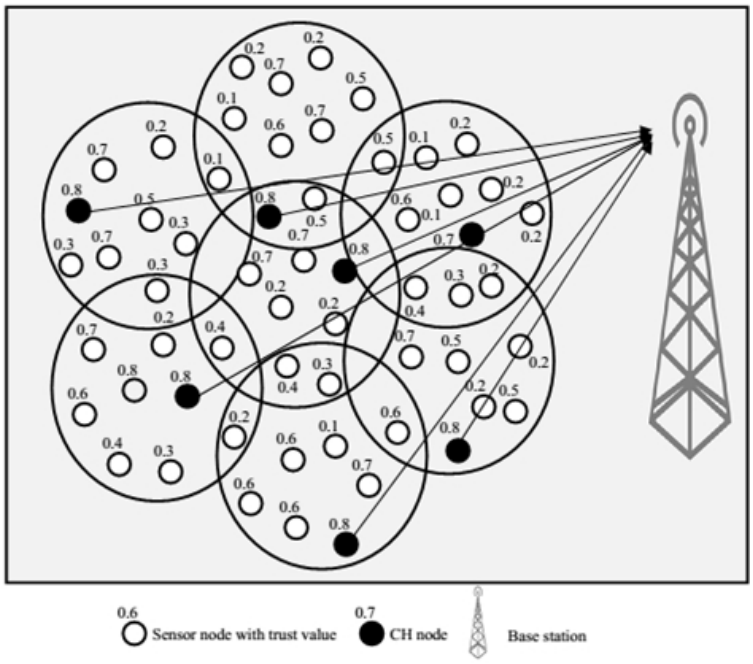

Fig. 1 *Network model of proposed OC-KMS with example trust values.*

on upon some passing anticipation of station keeping reactions yet advances their possible and repeat. Creature movement is the fairly long-confine change of people, by and large talking on a typical begins. It is an inevitable ponder that can be found in all enormous creature parties, for example, birds, mammals, fish, reptiles, amphibians, insects, and crustaceans. Modified animal Diaspora (MAD) optimization algorithm can be divided into Diaspora process and updating process. The animal Diaspora process computes the groups of animal move from one position to next and the animal update process computes position changed animals are updated by the probabilistic method. The MAD algorithm with the Diaspora process and population updating process are used to compute a satisfactory solution. The proposed algorithm used a new migration process by establishing a living area by the best fitness value owned animal and animals migrate from current locations into this new living area to simulate animal Diaspora process. We consider N animals that live in living area, some individuals move randomly and their position updated, and then we calculate the best position of animals by fitness function and record it. But the amount of food or water gradually diminished as the time wore on, and some animals migrate from the current areas which have no food and water to a new area with abundant food and water.

The proposed MAD algorithm begins with an initialization process, for this work, we consider the animal as sensor nodes and their position as network position. Let set of N sensor nodes and their positionsare $P_1, P_2, P_3, \ldots, P_N$; each animal position P_i is a $1 \times (n \times d)$-dimensional vector, where n the number of clusters

and d is the dimension of the testset. The clusters $P_i^* = (p_{i_1}, p_{i_2} \ldots p_{i_d})$, where $i = 1, 2, \ldots, n$; each cluster is $1\times$ D-dimensional vector, and the lower bound of the centers is the minimum of each column in test set $t_{n\times d}$, denotes $t_l = \min(t_1, t_2, \ldots, t_d)$, and the upper bound of the centers is $t_u = \max(t_1, t_2, \ldots, t_n)$. Sensor nodes are randomly and uniformly distributed between the pre-specified lower initial parameter bound l and the upper initial parameter bound u. Once the neighborhood topology has been constructed, we select one neighbor randomly and update the position of the individual according to this neighbor as follows:

$$p_{i,j} = t_{l_j} + r_{i,j}[0,1] \cdot \left(t_{u_j} - t_{l_j}\right), \tag{1}$$

where $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, n \times d$, $r_{i,j}[0,1]$ represents the random numbers between 0 to 1. During the Diaspora process, because of nodes movement in the network area, some parts of the networks are lacking due to the condition change, and some nodes moving from the current position to new position depends on moving action.During the updating process, the algorithm computes how nodes leave the cluster and some join in the new population. Individuals will be replaced by some new nodes with a probability P_{new}. The probability is used according to the quality of the fitness. We sort fitness in descending order, so the probability of the individual with best fitness is 1/N and the individual with worst fitness, by contrast, is 1. After compute the new solution $p_{i,j+1}$, it will be evaluated and compared with the $p_{i,j}$ and we choose the individual with a better objective fitness and denotes as follows:

$$P_i = \begin{cases} p_{i,j}; & \text{if } f(i,j) \text{ is better than } f(i,j+1) \\ p_{i,j+1}; & \text{otherwise} \end{cases}. \tag{2}$$

In this work, we use Rastrigin's function for fitness computation and define as follows:

$$f(i,j) = \sum_{i=1}^{n} \left[p_i^2 - 10\cos(2\pi p_i) + 10\right], \tag{3}$$

where the range variables denotes as $-5.12 \leq p_i \leq 5.12$. Rastrigin's function is based on cosine modulation to produce many local minima.

4.1.2 Cluster Head (CH) selection using JAYA trust model

JAYA is a new trust inference model, which produce optimal solutions for constrained and unconstrained optimization problems. Not in any manner like other people based heuristic algorithms, JAYA has no count specific controlling parameter, and incorporates only the two customary controlling parameters of masses size and the amount of times. The upgrade technique of this methodology is evoked on the commence of the likelihood that the plan chosen for a specific issue need to advance toward the perfect game plan and evade the menial game plan. The basic JAYA algorithm applied for the CH selection among cluster members in the cluster for optimizes the matching criteria. Hence, the optimum penetration has been provides the best match values with the limited search space. The formulation of objective problem can be expressed as:

$$\text{Minimize P}(y); y = 1, 2, 3 \ldots \tag{4}$$

Subject to energy consumption (P(1)), received signal strength (P(2)), and mobility (P(3)) and the proposed JAYA trust model applied to solve the problem. The details of constraints are as follows:

The energy consumption is derived from basic energy model, which consider both the transmitter and receiver part energy requirements. The energy consumption of wireless node depends on the amount of the data and distance to be sent. The energy consumption of a node is proportional to square of distance (D^2) when the propagation distance (D) less than the threshold distance (D_0), otherwise it is proportional to D^2. The total energy consumption of each node in the network for transmits and receives n bit data packet.

$$E_{\text{total}} = \text{FFE}(n,d) + \text{FRE}\,(n)\,, \tag{5}$$

where FFE (n,d) and FRE(n) are energy consumption of transmitting and receiving node.

$$\text{FFE}\,(n,d) = \begin{cases} n \times E_{\text{elec}} + n \times \varepsilon_{\text{fs}} \times D^2; & \text{if } D < D_0 \\ n \times E_{\text{elec}} + n \times \varepsilon_{\text{mp}} \times D^4; & \text{if } D \geq D_0 \end{cases}, \tag{6}$$

$$\text{RFE}\,(n) = n \times E_{\text{elec}}, \tag{7}$$

where E_{elec} the energy is dissipated per bit to run the transmitter or receiver circuit, amplification energy for free space model $\left(\varepsilon_{\text{f}s}\right)$ and for multi-path model $\left(\varepsilon_{\text{mp}}\right)$ depends on the transmitter amplifier model and D_0 is the threshold transmission distance. The considered all attacks are responsible for the energy consumption.

Received signal strength (RSS) is determined by the distance and transmission energy, if the node transmits frame/packet with energy FFE (n,d), the nodes received signal strength RSS, with the distance of D, can be expressed as follows:

$$\text{RSS} = \frac{\text{FFE}\,(n,d)}{4\pi D_i^2} + T_{a,a_1/a_2}. \tag{8}$$

Node mobility is the distance and relative speed determine the speed accurately according to the current sampled signal strength, sample points are selected which meet constrain $\Delta t_1 = \Delta t_2 = \Delta t$, but the sample domain may have no such points. Different reference points are used to approximate nodes' actual received signal strength. The distance D_{i1}, D_{i2} and D_{i3} can be obtained from Eq. (8), and the modified distance is computed from the cosines laws as follows:

$$D_{i1}^2 = D_{i2}^2 + a_1 a_2^2 - 2D_{i2} \cdot a_1 a_2 \cdot \cos\,(\alpha)\,, \tag{9}$$

$$D_{i3}^2 = D_{i3}^2 + a_1 a_2^2 - 2D_{i2} \cdot a_1 a_2 \cdot \cos\,(\beta)\,. \tag{10}$$

The current position of node is a, and can move to a_1 and a_2 in two reference points respectively. Consider $\cos\,(\alpha) = -\cos\,(\beta)$ and simply above equation to compute velocity (v) as follows:

$$2a_1 a_2^2 = D_{i1}^2 + D_{i3}^2 - 2D_{i2}^2, \tag{11}$$

$$v = \sqrt{\frac{2\,(D_{i1}^2 + D_{i3}^2 - 2D_{i2}^2)}{2\Delta t}}. \tag{12}$$

The movement duration for mobile node from current position a to the moved position a_1 or a_2 is expressed as the distance $T_{a,a_1/a_2}$ divided the node's velocity and it can obtain by sign law as follows:

$$T_{a,a_1/a_2} = \frac{R \cdot \sin \vartheta}{\sin \beta \cdot v}. \tag{13}$$

Applied Eq. (9) in (10) and we have,

$$T_{a,a_1/a_2} = \frac{\Delta t \cdot R \cdot \sin \vartheta}{\sin \beta \cdot \sqrt{\frac{\left(D_{i1}^2 + D_{i3}^2 - 2D_{i2}^2\right)}{2}}}. \tag{14}$$

The JAYA trust model begins with the initialization process in which we define the population size, design variables, and termination.Then compute the values of goal functions for the initial status, which energy consumption, RSS, and mobility, using Eqs. (5), (7), and (10) respectively. Then create an initial random population based on the defined controlling parameters within the pre-specified limits of design variables. The population $\mathbf{P}(y)$ is formulated as follows:

$$\mathbf{P}\left(y\right) = \begin{bmatrix} p_1\left(1\right) & p_1\left(2\right) & \cdots & p_1\left(n\right) \\ p_2\left(1\right) & p_2\left(2\right) & \cdots & p_2\left(n\right) \\ \vdots & \vdots & \vdots & \vdots \\ p_m\left(1\right) & p_m\left(2\right) & \cdots & p_m\left(n\right) \end{bmatrix}, \tag{15}$$

where n is the number of control variables, whereas m is the number of cluster members in the network of any iteration i. Let the best candidate best obtains the best value of $\mathbf{P}\left(1\right)_b$ in the entire candidate solutions and the worst candidate worst obtains the worst value of $\mathbf{P}\left(1\right)_w$ in the entire candidate solutions. If $\mathbf{P}_{m,n,i}$ is the value of n-th variable for the m-th candidate during i-th iteration can be written as follows:

$$\mathbf{P}^{\tau}_{m,n,j} = \mathbf{P}_{m,n,i} + \mathrm{r}_{m,1,i}\left(\mathbf{P}_{m,b,i} - |\mathbf{P}_{m,n,i}|\right) - r_{m,2,i}\left(\mathbf{P}_{m,w,i} - |\mathbf{P}_{m,n,i}|\right), \tag{16}$$

where $r_{m,1,i}$ and $r_{m,2,i}$ is the random numbers between 0 to 1. For details, let assume the $100 \times 100\,\mathrm{m}^2$ network size with 100 nodes in the network and we consider the candidates of cluster as 25 members. From this, total population size is $m = 25$, and design variables as $n = 3$. The physical elements can be described as follows:

$$\mathbf{P} = \begin{bmatrix} p_1\left(1\right) & p_1\left(2\right) & p_1\left(3\right) \\ p_2\left(1\right) & p_2\left(2\right) & p_2\left(3\right) \\ \vdots & \vdots & \vdots \\ p_{25}\left(1\right) & p_{25}\left(2\right) & p_{25}\left(3\right) \end{bmatrix}. \tag{17}$$

Run control stream program for every contender approach and figure the estimation of target cutoff that relates to each philosophy. See the best and most detectably accursed game-plans among the contender plots. In light of the best and most unmistakably dazzling diagrams, change each and every without question approach. For every restored plan, if any design variable upper/segregate down most cleared

point is hurt, supplant the evaluated a focal reason with past what many would consider conceivable. For each iteration, look at the target work values for the past and upheld approach. See the maintained layout in the event that it is better than the past value. Something else, keep the past value. Stop and report the ideal system if the end presentation is refined. The fitness is computed using Eq. (3).

4.2 Key management using certificate-less signcryption algorithm

Properties of signcryptionalgorithm: Certificate-lesssigncryptionalgorithm allows to simultaneously performing the functions of both digital signature and encryption. In this work, we have proposed a new algorithm, ECC combined with identity and Korean certificate-based digital signature algorithm. Confidentiality, integrity, non-repudiation and authentication are the important requirements for many cryptographic applications. The proposed signcryption scheme starts with an initial setup followed by extract, signcryption, and unsigncryption phase. The security input parameters are defined using key management system in setup phase and define an elliptic curve E over finite field $F_p$with a generator groups G1 and G2 of prime order p, an admissible bilinear pairing e: $\mathrm{G}_1 \cdot \mathrm{G}_1 \rightarrow \mathrm{G}_2$. Two hash functions are also defined as $H_1 : \{0,1\}^* \rightarrow Z_p$ and $H_2 : \{0,1\}^* \rightarrow \{0,1\}^*$. The private key generator generates master key (mk) is kept secret and system parameter (P_s) made public. In extraction phase, private key generator computes the private key (d_i) based on given identity (I). Signcryption handles the source node identity (I_s) and private key (d_i), destination node identity (I_d) and a message (M) to generate the source outputs and it is forward to the cipher text (CT). The source node identity (I_s), the destination node identity (I_d) and private key and the cipher text (CT) are used in the receiver side to recover the original message.

Let an identity be a bit string of length n_u, and let I_i be the i-th bit of identity and define the $U_i \subset \{1, 2, \ldots, n_u\}$ set of indices. A private key (d_i) for identity is generated as follows:

$$d_i = (d_{i_1}, d_{i_2}) = \left(mk \left(e \times \prod_{i \in U_i} Z_n \right)^{r_i, mk_i} \right). \tag{18}$$

Therefore, the sender and the receiver identity with private keys are as follows:

$$d_{i_s} = (d_{s_1}, d_{s_2}) = \left(mk \left(e \times \prod_{i \in U_i} Z_{n_s} \right)^{r_s, mk_s} \right), \tag{19}$$

$$d_{i_d} = (d_{d_1}, d_{d_2}) = \left(mk \left(e \times \prod_{i \in U_i} Z_{n_d} \right)^{r_d, mk_d} \right). \tag{20}$$

Then we can validate the public key by using the following equation:

$$P_k = d_i + H_1 \left(d_{i_s} || U_i || e || d_i \right) \cdot U_i. \tag{21}$$

The detailed procedure of thisalgorithm described as follows:

In signcryption, the adversary submits a source node and destination node identities and a message, and the challenger responds with the cipher text under the source private key and the destination public key. Suppose the sender (S) with identity I_s wants to send message $M \in (0,1)^n$ to the destination (D) with identity I_d.

1. Compute $S_1 = e \cdot n_u$
2. Compute $x = Z_n^{\max(r_s, r_d)}$
3. Compute $y = \mathbf{M} \cdot H_1$
4. Compute $S_2 = (d_{i_d})^{P_k}$
5. Compute $S_3 = \left(2 \times \prod_{i \in U_i} Z_n\right)^{r_s, mk_s}$
6. Compute $z = H_2(M, S_1, S_2, S_3, x + y)$
7. Compute $S_4 = (d_{i_d})^{P_k} + S_3 + \left(\mathbf{M}^{\mathrm{T}} \times \prod_{i \in U_i} Z_i\right)^r$.

Finally, forward the cipher text $CT = (S_1, S_2, S_3, S_4, y)$ to the destination node. In unsigncryption, the adversary submits a cipher text and a destination node identity, and the challenger decrypts the cipher text under the private key of the destination and verifies that the resulting decryption is a valid message/signature pair under the public key of the decrypted identity. Then, the challenger returns the message.

1. Compute $x = e(d_{i_s}, S_1) \cdot e(d_{i_d}, S_3)^{-1}$
2. Compute $\mathbf{M} = y \cdot H_1$
3. Compute $z = H_2(M, S_1, S_2, S_3, x + y)$
4. Verify the message if and only if the following equality holds as follows:

$$e(S_4, x) = e\left(y \times \prod_{i \in U_i} Z_n, S_1\right) e\left(\mathbf{M}^{\mathrm{T}} \times \prod_{i \in U_i} Z_i, S_1\right). \tag{22}$$

5. Simulation result

The Network Simulator (NS2) tool is used to simulate the proposed key management system for WSNs. A network of 100, 200, 300, 400 and 500 sensor nodes placed randomly within a 1000×1000 meter network size isconsidered for this experiment and different network layer attacks are used for this experimentations.Radio propagation range for each node is 250 meters and channel capacity is 2 Mbits/sec. The IEEE 802.11 is used as the medium access control (MAC) protocol. The total simulation time of each test will set as 100 seconds. The node mobility uses the

random waypoint model. In the following tests, network layer attacks can launch that are black hole (BH), worm hole (WH), gray hole (GH), rushing, and key compromising attacks.The simulation settings and parameters are summarized in Tab. I. The performance of the proposed OC-KMS system is discussed with existing DKMM system [35] in terms of delay, delivery ratio, energy consumption, number of keys used, network lifetime, and throughput.The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations. Delivery ratiois the ratio of the number of packets received successfully and the total number of packets transmitted. Energy consumption is the amount of energy consumed by the source or relay nodes to transmit the data packets to the destination. The storage space of sensor network nodes is limited, so it is necessary to reduce consumption of nodes key storing under the condition of safety. Network lifetime is time until the first sensor node or group of sensor nodes in the network runs out of energy. The throughput is the amount of data that can be sent from the sources to the destination.

Parameter	Parameter values
Number of nodes	40, 80, 120, 160, and 200
Number of attacks	5, 10, 15, 20, and 25
Simulation area	$1000 \times 1000\,\mathrm{m}^2$
Node mobility	10 m/s
MAC protocol	IEEE 802.11
Transmission range of node	250 m
Channel capacity	2 Mb/s
Initial energy of nodes	100 joules
Traffic type	CBR
Packet size	512 bytes
Simulation Time	100 seconds

Tab. I *Simulation parameters.*

The three different testing scenarios are used to analyze the performance of proposed key management system and given in Tab. II.

Scenarios	Number of nodes	Number of attacks	Number of rounds
1	40–200	5	100
2	200	5–25	100
3	200	5	40-200

Tab. II *Test scenarios.*

5.1 Scenario 1-varying number of nodes

In the first experiment, the performance of proposed OC-KMS is analyzed by varying number of nodes in the network with the fixed number attack as 5 and optimization algorithm iteration level as 100. We plot the delay performance with respect to the varying nodes in Fig. 2 and is clearly depicts the delay of proposed OC-KMS is very low compared to the existing DKMM system, but it is increased with respect to the increase of a number of nodes.We plot the delivery ratio performance with respect to the varying nodes in Fig. 3 and is clearly depicts the delivery ratio of

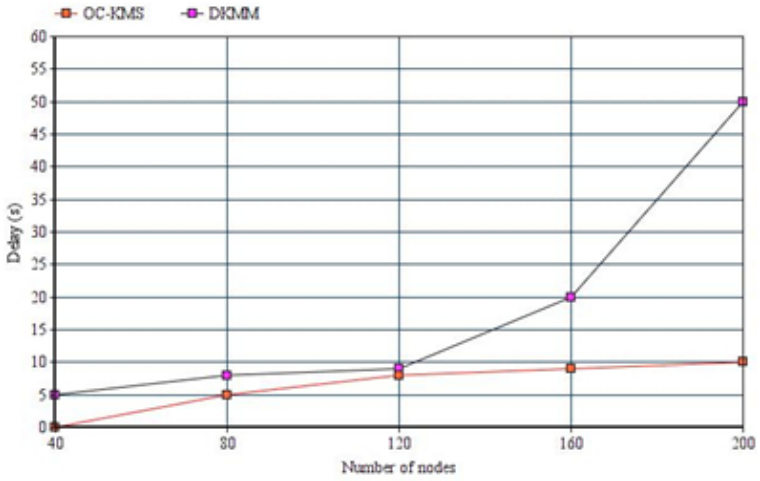

Fig. 2 *Delay comparison between proposed OC-KMS and DKMM system for varying number of nodes.*

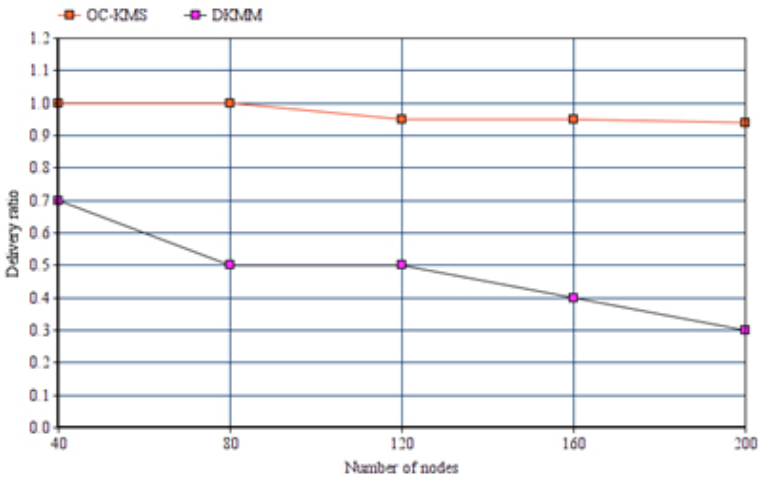

Fig. 3 *Delivery ratiocomparison between proposed OC-KMS and DKMM system for varying number of nodes.*

proposed OC-KMS is very high compared to the existing DKMM system, but it is slightly decreased with respect to the increase of a number of nodes.We plot the energy consumption performance with respect to the varying nodes in Fig. 4 and is clearly depicts the energy consumption of proposed OC-KMS is very low compared to the existing DKMM system, but it is increased with respect to the increase of a number of nodes.We plot the total number of keys with respect to the varying nodes in Fig. 5 and is clearly depicts the number of keys of proposed OC-KMS is very low compared to the existing DKMM system.We plot the network lifetime with

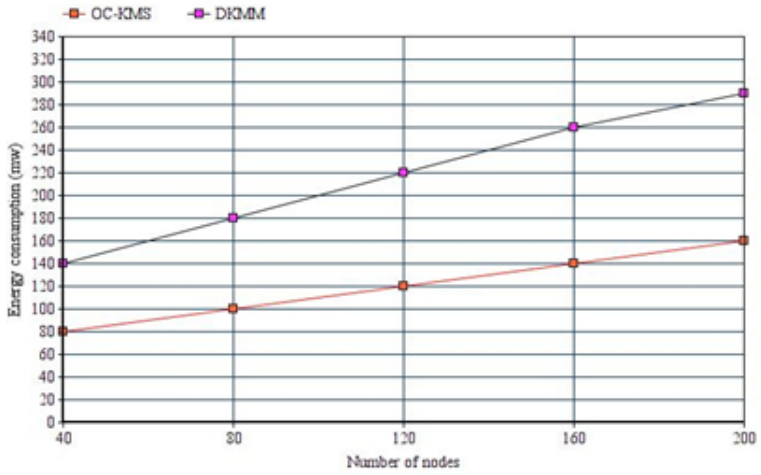

Fig. 4 *Energy consumptioncomparison between proposed OC-KMS and DKMM system for varying number of nodes.*

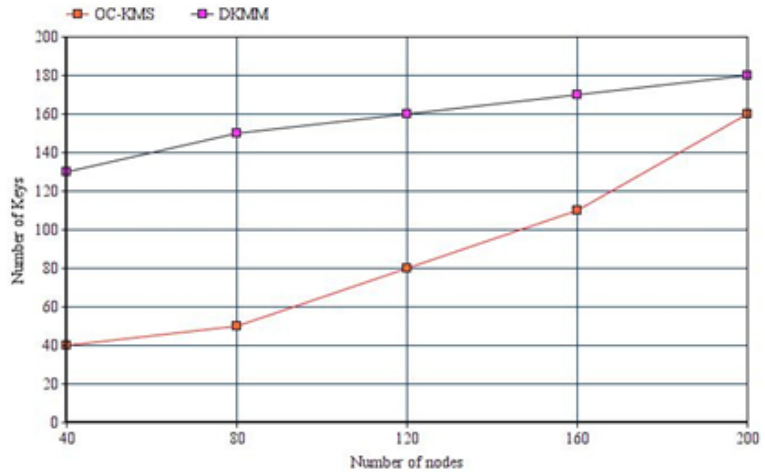

Fig. 5 *Total number of keys comparison between proposed OC-KMS and DKMM system for varying number of nodes.*

respect to the varying nodes in Fig. 6 and is clearly depicts the network lifetime of proposed OC-KMS is very high compared to the existing DKMM system.We plot the throughput performance with respect to the varying nodes in Fig. 7 and is clearly depicts the throughput of proposed OC-KMS is very high compared to the existing DKMM system, but it is decreased with respect to the increase of a number of nodes.

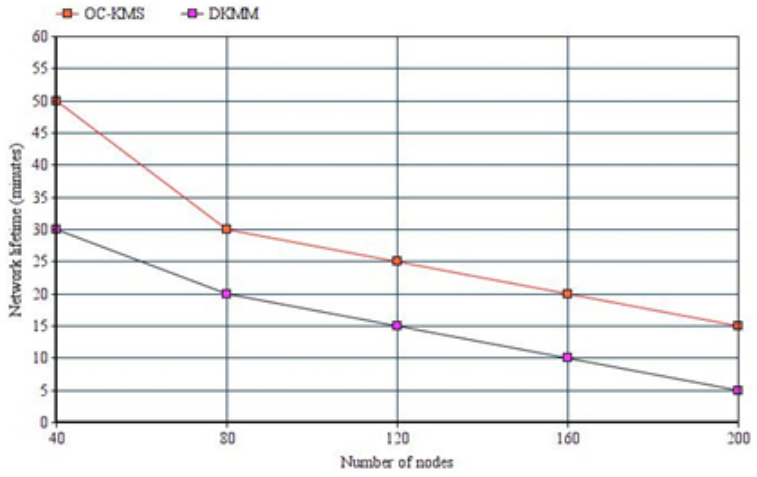

Fig. 6 *Network lifetimecomparison between proposed OC-KMS and DKMM system for varying number of nodes.*

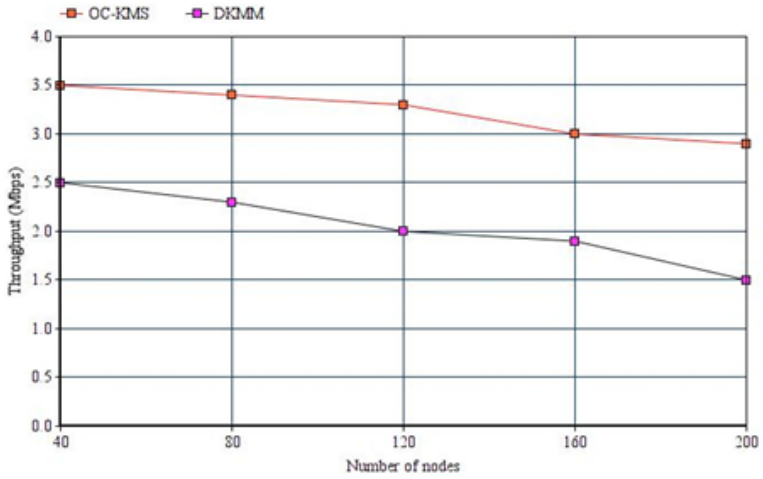

Fig. 7 *Throughput comparison between proposed OC-KMS and DKMM system for varying number of nodes.*

5.2 Scenario 2-varying number of attacks

In the first experiment, the performance of proposed OC-KMS is analyzed by varying number of attacks in the network with the fixed number nodes as 200 and an algorithm iteration level as 100. We plot the delay performance with respect to the varying attacks in Fig. 8 and is clearly depicts the delay of proposed OC-KMS is very low compared to the existing DKMM system, but it is increased with respect to the increase of a number of attacks. We plot the delivery ratio performance with respect to the varying attacks in Fig. 9 and is clearly depicts the delivery

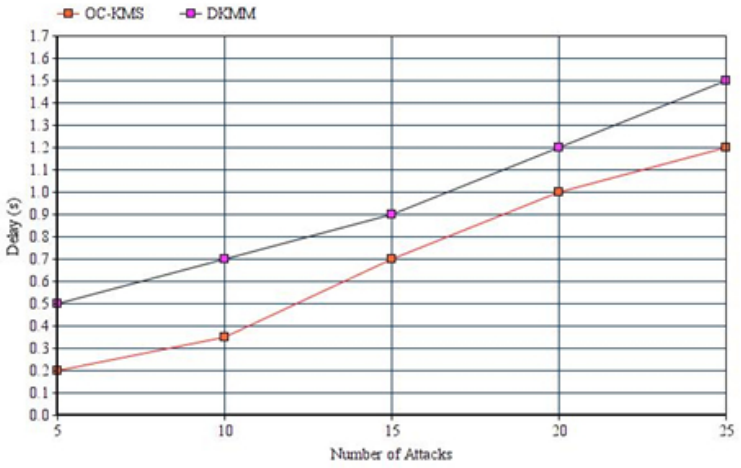

Fig. 8 *Delay comparison between proposed OC-KMS and DKMM system for varying number of attacks.*

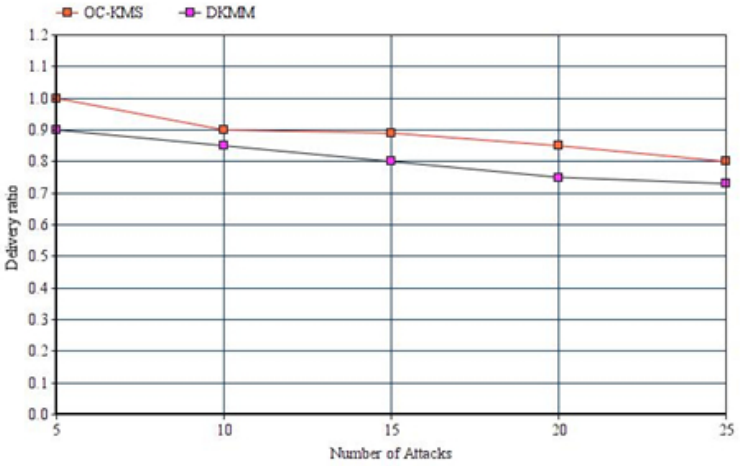

Fig. 9 *Delivery ratio comparison between proposed OC-KMS and DKMM system for varying number of attacks.*

ratio of proposed OC-KMS is very high compared to the existing DKMM system, but it is slightly decreased with respect to the increase of a number of attacks. We plot the energy consumption performance with respect to the varying attacks in Fig. 10 and is clearly depicts the energy consumption of proposed OC-KMS is very low compared to the existing DKMM system, but it is increased with respect to the increase of a number of attacks. We plot the total number of keys with respect to the varying attacks in Fig. 11 and is clearly depicts the number of keys of proposed OC-KMS is very low compared to the existing DKMM system. We

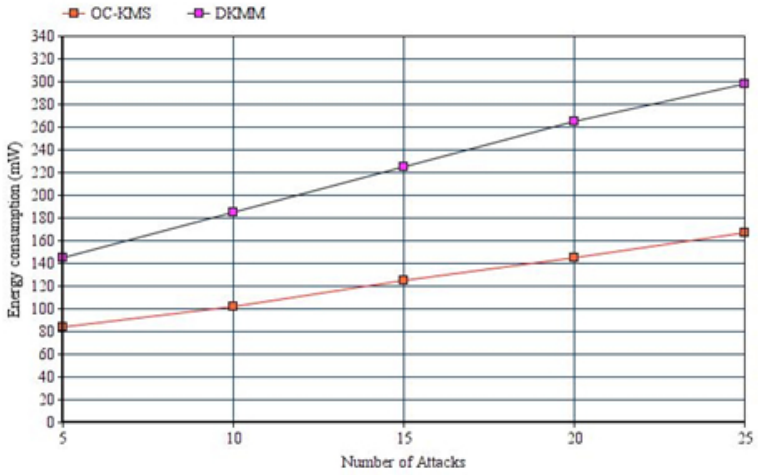

Fig. 10 *Energy consumption comparison between proposed OC-KMS and DKMM system for varying number of attacks.*

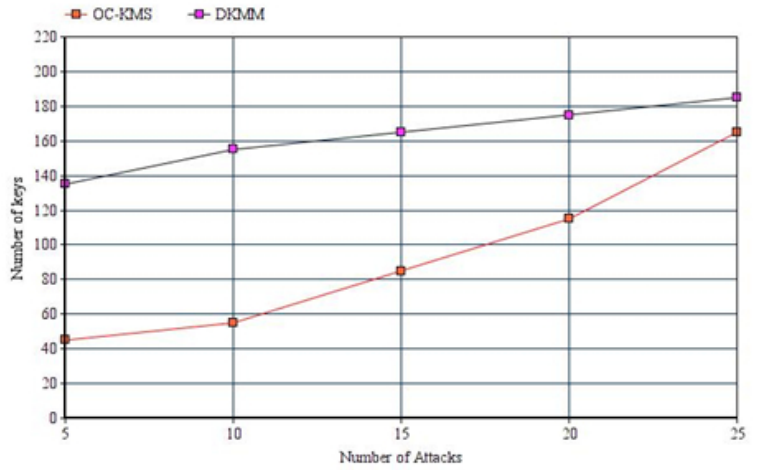

Fig. 11 *Total number of keys consumption comparison between proposed OC-KMS and DKMM system for varying number of attacks.*

plot the network lifetime with respect to the varying attacks in Fig. 12 and is clearly depicts the network lifetime of proposed OC-KMS is very high compared to the existing DKMM system. We plot the throughput performance with respect to the varying attacks in Fig. 13 and is clearly depicts the throughput of proposed OC-KMS is very high compared to the existing DKMM system, but it is decreased with respect to the increase of a number of attacks.

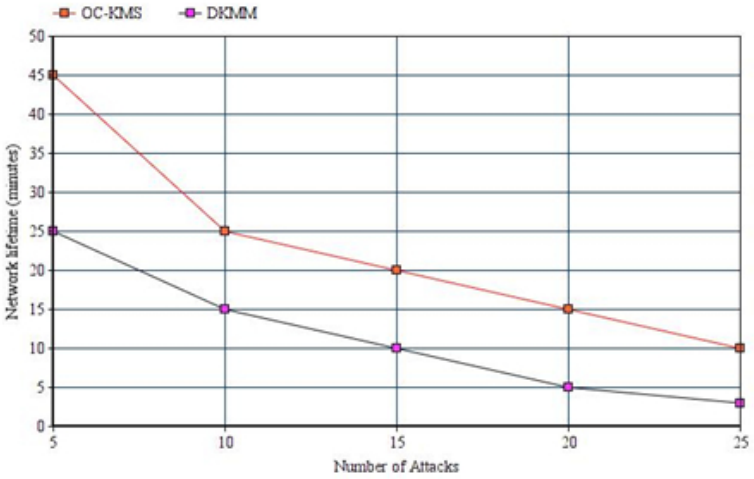

Fig. 12 *Network lifetime consumption comparison between proposed OC-KMS and DKMM system for varying number of attacks.*

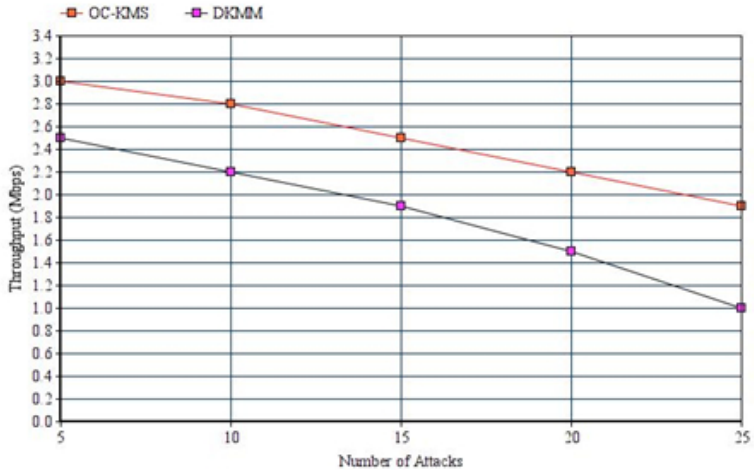

Fig. 13 *Throughput comparison between proposed OC-KMS and DKMM system for varying number of attacks.*

5.3 Scenario 3-varying number of rounds

In this experiment, the performance of proposed OC-KMS is analyzed by varying number of rounds with the fixed number nodes as 200 and attacks as 5. We plot the number of times the CH nodes will change with respect to the varying number of rounds in Fig. 14 and is clearly depicts the CH node change of proposed OC-KMS is high compared to the existing DKMM system. The CH change will maintain the network lifetime of proposed system.

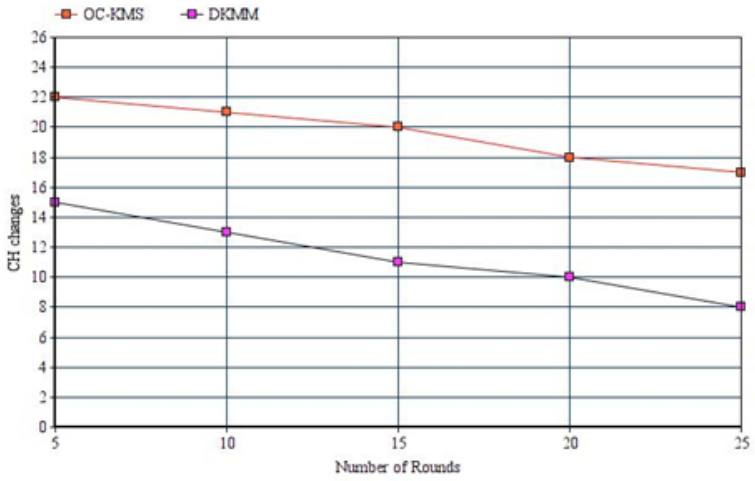

Fig. 14 *Comparison of CH change between proposed OC-KMS and DKMM system for varying number of rounds.*

6. Conclusion

In this paper, we have proposed an optimal cluster based key management system OC-KMS for WSNs. We first perform the clustering using modified animal Diaspora (MAD) optimization algorithm and JAYA trust model. The combined optimization and trust model improves the energy consumption and first level securities in terms of enter/leave in/from cluster. Then certificate-less syncryption algorithm utilized to enhancesthe key management.The proposed OC-KMS keeps the low energy consumption and maximize the network lifetime to overcome the poor resilience against network layer attacks. The advantages of high security in OC-KMS proved through comparison with other schemes in terms of delay, delivery ratio, energy consumption, number of keys used, network lifetime, and throughput.

References

[1] LARA-CUEVA R.A., GORDILLO R., VALENCIA L., BENÍTEZ D.S. Determining the main CSMA parameters for adequate performance of wsn for real-time volcano monitoring system applications. *IEEE Sensors Journal*, 2016, 17(5), pp. 1493–1502, doi: 10.1109/JSEN.2016.2646218.

[2] PRAYATI A. Wireless Technology Applications in Environment and Health: Network Design Challenges. *IEEE Latin America Transactions*, 2012, 10(3), pp. 1853–1855, doi: 10.1109/TLA.2012.6222594.

[3] ALBERT D.J., MORSE S.P., Combatting software piracy by encryption and key management. *Computer*, 1984, 4, pp. 68–73, doi: 10.1109/MC.1984.1659112.

[4] GREENLEE M. Requirements for key management protocols in the wholesale financial services industry. *IEEE Communications Magazine*, 1985, 23(9), pp. 22–28, doi: 10.1109/MCOM.1985.1092640.

[5] SETHI K.K., MISHRA D.K., SOLANKI G., MISHRA B. Key Issues of Security and Integrity in Third Party Association Rule Mining. In Emerging Trends in Engineering and Technology (ICETET), *2009 2nd International Conference on IEEE*, 2009, pp. 337–340, doi: 10.1109/ICETET.2009.136.

[6] DOAN P.T.H., ARCH-INT N., ARCH-INT S., Improving key concept extraction using word association measurement. *In Information Technology and Electrical Engineering (ICITEE), 2015 7th International Conference on IEEE*, 2015, pp. 403–407, doi: 10.1109/ICITEED.2015.7408980.

[7] WALKER J., HON S.E., Supplier quality improvement-the key to long-term quality relationships. *IEEE Journal on Selected Areas in Communications*, 1988, 6(8), pp. 1322–1325, doi: 10.1016/j.ejor.2017.05.044.

[8] DONOVAN J.J. Opportunities and challenges for the key executive. *IEEE Circuits and Devices Magazine*, 1988, 4(2), pp. 16–21, doi: 10.1109/101.935.

[9] ESCHENAUER L., GLIGOR V.D., A key-management scheme for distributed sensor networks. *In Proceedings of the 9th ACM Conference on Computer and Communications Security. ACM*, 2002, pp. 41–47, doi: 10.1145/586110.586117.

[10] HUANG H.F. A pairwise key pre-distribution scheme for wireless sensor network. *In International Conference on Intelligence and Security Informatics Springer*, Berlin, Heidelberg, 2008, pp. 77–82. doi: 10.1007/978-3-540-69304-8_9.

[11] ZHU S., SETIA S., JAJODIA S., LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 2006, 2(4), 500–528, doi: 10.1145/1218556.1218559.

[12] YOUNIS M.F., GHUMMAN K., ELTOWEISSY M. Location-aware combinatorial key management scheme for clustered sensor networks. *IEEE transactions on parallel and distributed systems*, 2006, 17(8), pp. 865–882, doi: 10.1109/TPDS.2006.106.

[13] PANJA B., MADRIA S.K., BHARGAVA B. Energy and communication efficient group key management protocol for hierarchical sensor networks. In Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. *IEEE International Conference on IEEE*. 2006, 1, pp. 8, doi: 10.1109/SUTC.2006.1636204.

[14] ELTOWEISSY M., MOHARRUM M., MUKKAMALA R. Dynamic key management in sensor networks. *IEEE Communications magazine*, 2006, 44(4), pp. 122–130, doi: 10.1109/MCOM.2006.1632659.

[15] ÇAMTEPE S.A., YENER B. Combinatorial design of key distribution mechanisms for wireless sensor networks. *IEEE/ACM Transactions on networking*, 2007, 15(2), pp. 346–358, doi: 10.1109/TNET.2007.892879.

[16] LU K., QIAN Y., GUIZANI M., CHEN H.H. A framework for a distributed key management scheme in heterogeneous wireless sensor networks. *IEEE Transactions on Wireless Communications*, 2008, 2(7), pp. 639–647, doi: 10.1109/TWC.2008.060603.

[17] YU Z., GUAN Y. A key management scheme using deployment knowledge for wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 2008, 19(10), pp. 1411–1425, doi: 10.1109/TPDS.2008.23.

[18] KWON T., LEE J., SONG J. Location-based pairwise key predistribution for wireless sensor networks. *IEEE transactions on wireless communications*, 2009, 8(11), doi: 10.1109/TWC.2009.090183.

[19] DU X., GUIZANI M., XIAO Y., CHEN H.H. Transactions papers a routing-driven Elliptic Curve Cryptography based key management scheme for Heterogeneous Sensor Networks. *IEEE Transactions on Wireless Communications*, 2009, 8(3), pp. 1223–1229, doi: 10.1109/TWC.2009.060598.

[20] YU C.M., LU C.S., KUO S.Y. Noninteractive pairwise key establishment for sensor networks. *IEEE Transactions on Information Forensics and Security*, 2010 5(3), pp. 556–569, doi: 10.1109/TIFS.2010.2050140.

[21] ALAGHEBAND M.R., AREF M.R. Dynamic and secure key management model for hierarchical heterogeneous sensor networks. *IET Information Security*, 2012, 6(4), pp. 271–280, doi: 10.1049/iet-ifs.2012.0144.

[22] WILHELM M., MARTINOVIC I., SCHMITT J.B., Secure key generation in sensor networks based on frequency-selective channels. *IEEE Journal on Selected Areas in Communications*, 2013, 31(9), pp. 1779–1790, doi: 10.1109/JSAC.2013.130911.

[23] BECHKIT W., CHALLAL Y., BOUABDALLAH A., TAROKH V. A highly scalable key pre-distribution scheme for wireless sensor networks. *IEEE Transactions on Wireless Communications*, 2013, 12(2), pp. 948–959, doi: 10.1109/TWC.2012.010413.120732.

[24] YA-NAN L., JIAN W., HE D., LI-JUN S. Intra-cluster key sharing in hierarchical sensor networks. *IET Wireless Sensor Systems*, 2013, 3(3), pp. 172–182, doi: 10.1049/iet-wss.2012.0155.

[25] SEO S.H., WON J., SULTANA S., BERTINO E. Effective key management in dynamic wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 2015, 10(2), pp. 371–383, doi: 10.1109/TIFS.2014.2375555.

[26] GANDINO F., MONTRUCCHIO B., REBAUDENGO M. Key management for static wireless sensor networks with node adding. *IEEE Transactions on Industrial Informatics*, 2014, 10(2), pp. 1133–1143, doi: 10.1109/TII.2013.2288063.

[27] LALITHA T., JAYAPRABHA S. Mobility based key management security scheme for wireless sensor networks. *Wireless Personal Communications*, 2016, 87(2), pp. 349–367, doi: 10.1007/s11277-015-2872-6.

[28] ANITA E.M., GEETHA R., KANNAN E. A novel hybrid key management scheme for establishing secure communication in wireless sensor networks. Wireless Personal Communications, 2015, 82(3), pp. 1419–1433, doi: 10.1007/s11277-015-2290-9.

[29] MESSAI M.L., SEBA H., ALIOUAT M. A lightweight key management scheme for wireless sensor networks. *The Journal of Supercomputing*, 2015, 71(12), pp. 4400–4422, doi: 10.1007/s11227-015-1534-5.

[30] SUN X., WU X., HUANG C., XU Z., ZHONG J. Modified access polynomial based self-healing key management schemes with broadcast authentication and enhanced collusion resistance in wireless sensor networks. *Ad Hoc Networks*, 2016, 37, pp. 324–336, doi: 10.1016/j.adhoc.2015.08.027.

[31] KUMARI S., LI X., WU F., DAS A. K., ARSHAD H., KHAN M.K. A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps. *Future Generation Computer Systems*, 2016, 63, pp. 56–75, doi: 10.1016/j.future.2016.04.016.

[32] GANDINO F., FERRERO R., MONTRUCCHIO B., REBAUDENGO M. Fast hierarchical key management scheme with transitory master key for wireless sensor networks. *IEEE Internet of Things Journal*, 2016, 3(6), pp. 1334–1345, doi: 10.1109/JIOT.2016.2599641.

[33] ZHAN F., YAO N., GAO Z., TAN G. A novel key generation method for wireless sensor networks based on system of equations. *Journal of Network and Computer Applications*, 2017, 82, pp. 114–127, doi: 10.1016/j.jnca.2017.01.019.

[34] ANZANI M., JAVADI H.H.S., MODIRIR V. Key-management scheme for wireless sensor networks based on merging blocks of symmetric design. *Wireless Networks*, 2017, pp. 1–13, doi: 10.1007/s11276-017-1509-y.

[35] ZHANG Y., ZHENG B., JI P., CAO J. A key management method based on dynamic clustering for sensor networks. *International Journal of Distributed Sensor Networks*, 2015, 11(7), pp. 763675. doi: 10.1155/2015/763675.

[36] CHALKIAS K., BALDIMTSI F., HRISTU-VARSAKELIS D., STEPHANIDES G. Two types of key-compromise impersonation attacks against one-pass key establishment protocols. *In International Conference on E-Business and Telecommunications*, Springer, Berlin, Heidelberg, 2007, pp. 227–238, doi: 10.1007/978-3-540-88653-2_17.

[37] LI X., ZHANG J., YIN M. Animal migration optimization: an optimization algorithm inspired by animal migration behavior. *Neural Computing and Applications*, 2014, 24(7-8), pp. 1867–1877, doi: 10.1007/s00521-013-1433-8.

[38] GUPTA B., AGRAWAL D.P., YAMAGUCHI S. (EDS.). Handbook of research on modern cryptographic solutions for computer and cyber security. *IGI Global*. 2016. doi: 10.4018/978-1-5225-0105-3.

[39] YU C., LI J., LI X., REN X., GUPTA B.B. Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram. *Multimedia Tools and Applications*, 2018, 77(4), pp. 4585–4608, doi: 10.1007/s11042-017-4637-6.

[40] ATAWNEH S., ALMOMANI A., AL BAZAR H., SUMARI P., GUPTA B. Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain. *Multimedia tools and applications*, 2017, 76(18), pp. 18451–18472, doi: 10.1007/s11042-016-3930-0.

[41] CAO N., LIU P., LI G., ZHANG C., CAO S., CAO G., YAN M., GUPTA B.B. Evaluation Models for the Nearest Closer Routing Protocol in Wireless Sensor Networks. *IEEE Access*. pp. 1–1, 2018. doi: 10.1109/ACCESS.2018.2825441.

[42] YU Z., GAO C. Z., JING Z., GUPTA B.B., CAI Q. A Practical Public Key Encryption Scheme Based on Learning Parity with Noise. *IEEE Access*, 2018. doi: 10.1109/ACCESS.2018.2840119.

[43] AL-QURISHI M., RAHMAN S.M.M., HOSSAIN M.S., ALMOGREN A., ALRUBAIAN M., ALAMRI A., AL-RAKHAMI M., GUPTA B.B. An efficient key agreement protocol for Sybil-precaution in online social networks. *Future Generation Computer Systems*, 84, pp. 139–148, 2018. doi: 10.1016/j.future.2017.07.055.