Secure And Efficient Cluster Based Routing Model For Wireless Sensor Network

Chaitra H.V, Ravikumar G.K

Abstract—recently wireless sensor network has be adopted across wide range of application such as Internet of Things (IoT) based healthcare, military domain etc. due to its low cost availability and ease of deployment. For such application efficient secure and energy efficient design is needed. For improving energy efficiency exiting model adopted cluster based routing model. However, it incurs energy overhead among cluster head. Therefore, efficient cluster selection algorithm is needed. This work present an energy efficient cluster selection algorithm using multi-objective function using enhanced Imperialist Competitive Algorithm. Further, for providing secure communication the existing model are designed using asymmetric cryptography such as RSA, and Diffe-Hellman etc. As a result, incurs communication overhead and increase packet processing delay. For overcoming research challenges this work present symmetric Elliptical curve cryptography (ECC model. The proposed secure and efficient symmetric based ECC (SESECC) attained significant performance in terms of communication overhead, packet processing time and lifetime.

Keywords— WSN, Clustering, Cryptography, Evolutionary Computing.

I. INTRODUCTION

Wireless sensor networks (WSNs) emerged as an enabling platform for a broad range of application areas owing to their low-cost, low-power, small size, and adaptability to the physical environment [1]. These unique features triggered the proliferation and adoption of WSNs in several domains including military, health, and environment, but also gave rise to unique security challenges that cannot be tackled using classical security mechanisms [2]. In particular, asymmetric cryptosystems provide a scalable solution for securing large scale WSNs; however, they are generally slow and lead to excessive energy and memory consumption. On the other hand, symmetric cryptosystems were shown to be superior in terms of speed and energy efficiency, but they demand novel and efficient mechanisms for key-establishment among sensor nodes [3], [4]. In principle, an efficient key establishment mechanism should result in a securely connected topology, i.e., a network where there exists a secure communication path (possibly multihop) between every pair of nodes allowing the exchange of data and control messages, while conforming to the typical limitations of WSNs. Also, it shall not assume knowledge of post-deployment configuration, since in most cases WSNs are deployed randomly in large numbers.

In [5], [6] conducted extensive survey and identified problem in attaining secure and energy efficient routing model for WSN.

For attaining secure routing design for WSN [7] surveyed various LEACH based secure routing model (both symmetric and asymmetric cryptography protocol). The survey shows, there is a need for new design that brings a good trade-off between energy efficiency and security requirement of future application such Wearable computing device [8], smart city [9], tactical internet [10], Bigdata [11], and internet-of-Things [12], [13], [14].

Efficient routing: LEACH based routing model performs very well for small network. However, for large network it is inefficient. Firstly, for enhancing routing, [15] presented an energy efficient design for large sensor network adopting fuzzy based clustering approach. Further, [16] presented a clustering design using type-2 fuzzy logic (T2FL). The model distributed load among sensor devices which aided in improving the lifetime of sensor network. However, lifetime performance is not efficient, the cluster head devices closer to the base station dies rapidly. To address, [17], [18] presented a hop and multi-hop based communication is presented. However, their model induces high communication overhead among hop node and cluster device due to channel contention and optimizing it is NP-deterministic. In [19] conducted extensive survey of meta-heuristic optimization algorithm such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO) and Imperialist Competitive Algorithm (ICA) to solve to solve energy efficiency and cluster head selection optimization issue (.i.e. NP-hard problem) in WSN. The outcome presented in [20] and [21] shows that ICA perform better than GA and PSO. They highlighted that GA can solve global optimization problems. However, they are easily trapped in a local optimal solution and their executions are time-consuming [22]. PSO has numerous complications, such as easily falling into the local optimum and premature convergence [23]. The ICA model presented in [21] adopted PSO to prevent colonies from moving beyond search space. However their model is not efficient for multi-objective problems.

Secure routing: Number of security and privacy mechanism adopting cryptography has been presented recently for WSN [24], [25], [26], and [27]. In [24] discussed the need for provisioning security for tracking, navigation and localization of sensor device for sensor network. Further, for provisioning security and privacy, in [25] assumed that due randomness nature of sensor device there exist connectivity issues among sensor device. As a result, sharing keys among communicating device is challenging under homogenous network. In [26] proposed signcryption scheme which is composed of two stage such as offline and the online signcrypt stages. They showed that identity-based cryptography (IBC) setup for transmitting packet to a gateway in a public key infrastructure (PKI) can reduce heavy verification loads on low- power sensor devices.

Manuscript published on 30 September 2019.
***Correspondence Author(s)**
Chaitra H.V, NMIT, Bangalore, India,
Dr.Ravikumar G.K, Professor, BGSIT, India,

Further, [27] presented a secure time synchronization protocol for WSN using bilinear pairing. There model reduced communication overhead over existing approach due to adoption of ECC rather than conventional PKI. However, to efficiently adopt ECC in WSN, it is important to authenticate the public keys. Otherwise, the WSN is susceptible to man-in-the-middle attacks. Public key authentication needs a PKI, to issue and revoke certificates and also requires sensor device to store, exchange, and verify these certificates [28]. The issuance of certificates, as well as storage, exchange, and verification operations incur storage, communication, and computation overheads, and as a result, they are inadequate for WSNs [29].

To overcome the research challenges in designing Secure and Efficient Cluster based Routing (SECR) model for WSN. For attaining, firstly, this work firstly present energy efficient cluster based routing design for WSN. This work presents multi-objective based clustering model for WSN. The multi-objective optimization (i.e., energy and connectivity) is carried for cluster head and hop node selection using modified ICA. Secondly, for provisioning security this work present a secure and efficient symmetric ECC (SESECC) for both inter and intra cluster communication. SESECC offers dynamic generation of Mutual Session Keys (MSKs) without need of digital certificate of PKI. MSK is then utilized to encrypt and decrypt packet in the secure channel among cluster member and cluster head. SESECC allows cluster member to maintain its MSKs with each cluster head and no need of maintaining keys like convention methods, and thus aid in reducing complexity of maintenance. Since our model use ECC [30], [31] message and computation overhead is reduced when compared to conventional model such as Diffe-Hellman and RSA based approaches. Hence, the SESECC can offers confidentiality of packet information with minimal overhead of computation and maintenance.

Contribution of research work are as follows:

- The proposed SESECC model brings a good tradeoffs between security and energy efficiency requirement of WSN.
- The novelty of work is designing ECC as symmetrical cryptographic model while maintaining good security.
- The SESECC reduces computation overhead and packet processing time compared with state-of-art model.
- The SESECC model improves lifetime of sensor network when compared with existing models.
- The SESECC model does not require the cluster head to manage keys of its member thus preserve privacy and anonymity of sensor network. Further, aid in reducing communication overhead and allow cluster head to have more members.

The paper organization is as follows: The proposed secure and efficient clustering based routing model are presented in Section two. The simulation results and the experimental study are presented in the penultimate section. The concluding remark and future work is discussed in the last section.

II. PROPOSED SECURE AND EFFICIENT CLUSTERING BASED ROUTING MODEL FOR WSN

This section present a secure and efficient symmetric ECC (SESECC) for cluster based WSN. Firstly, this work present a novel multi-objective imperialist competitive algorithm (ICA) for attaining energy efficient clustering design for WSN. Secondly, for provisioning secure communication over WSN, this work presented a novel symmetric ECC (SECC) model. The architecture of SESECC is shown in Fig. 1.

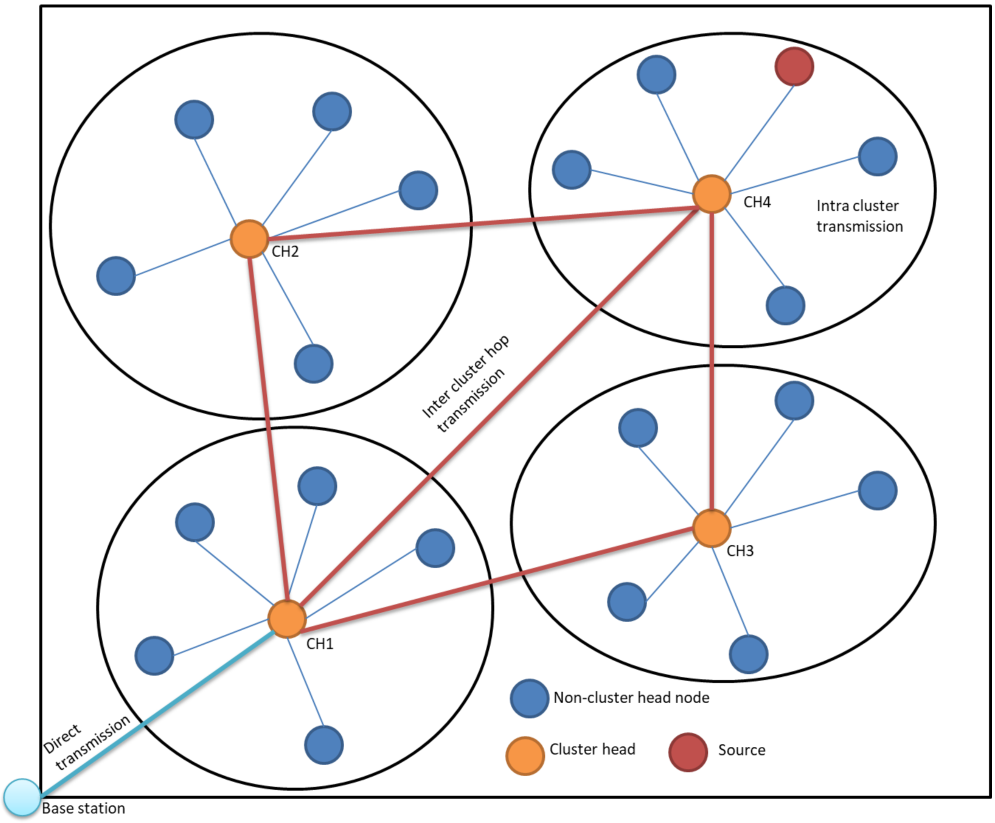

Fig. 1. Architecture of Proposed Model

a) *Multi-objective optimization problem description for energy efficient cluster based routing design:*

For cluster head selection, this work present a multi-objective Imperialist Competitive Algorithm (ICA) i.e., this work considers the **remaining energy and position** of sensor devices $\mathcal{K}$ as multi-objective function for cluster head $\mathcal{D}$ selection using ICA. This model is composed of setup and transmission stage. In setup stage, the cluster member, cluster head, route among the clusters and the base station are determined. In transmission stage, the cluster head collects and aggregate the data from its member and transfer this data to its **best optimized cluster** head/hop device toward base station.

The optimization problem for selecting cluster head can be described as follows

$$O_{\mathcal{D}} = \gamma * T_h^{\mathcal{D}} + (1-\gamma) * T_m^{\mathcal{D}} \tag{1}$$

where γ is the cost optimization constant, $T_h^{\mathcal{D}}$ is the ratio of cluster head mean remaining energy with respect to member device, $T_m^{\mathcal{D}}$ is the ratio of mean distance among non-cluster head and the sink to the mean distance among the cluster head and the base station. The optimization problem in eq. (1), comprises of two things, where γ is a constant which depicts the impact of $T_h^{\mathcal{D}}$ and $T_m^{\mathcal{D}}$ in computing cost optimization param $O_{\mathcal{D}}$.

The mean remaining energy of current round is computed as follows,

$$T_h^{\mathcal{D}} = \vec{L}_{\mathcal{D}} \Big/ \vec{L}_{\widetilde{\mathcal{D}}} \tag{2}$$

where $\vec{L}_{\widetilde{\mathcal{D}}}$ is the mean remaining energy of cluster member device and $\vec{L}_{\mathcal{D}}$ is the mean remaining energy of cluster head, $|\widetilde{\mathcal{D}}|$ and $|\mathcal{D}|$denotes the number of cluster member device and number cluster head devices respectively. The **sensor device with maximum $T_h^{\mathcal{D}}$ is selected as cluster head**. Similarly, The $T_m^{\mathcal{D}}$ is computed as follows,

$$T_m^{\mathcal{D}} = \vec{E}_{\widetilde{\mathcal{D}}} \Big/ \vec{E}_{\mathcal{D}} \tag{3}$$

where $e(s_x, \mathcal{S})$ represent the distance among base station $\mathcal{S}$ and node x. To improve the energy of sensor network, the objective function **$T_m^{\mathcal{D}}$ can be maximized to optimize better cluster formation and cluster head selection**.

To reduce the energy consumption of cluster device for inter cluster transmission, hop nodes (Cluster head) are selected to transmit data. The hop devices are selected based on following condition. Firstly, the cluster head and hop device must possess higher energy than normal sensor device. Secondly, the hop device should possess better location between base station and cluster head, in order to minimize energy consumption. To **reduce the computation cost among cluster head and hop nodes**, the cluster selects the neighbouring cluster head as its hop device.

The set of inter cluster hop device can be represented as $\mathbb{D} = \{\mathbb{D}_1, \mathbb{D}_2, \mathbb{D}_3, \dots, \mathbb{D}_u, \dots, \mathbb{D}_v\}$ and set of normal sensor devices as $\mathbb{S}$. The cost function for selection hop device for inter cluster transmission is given as follows

$$O_{\mathbb{D}} = \varphi * T_h^{\mathbb{D}} + (1-\varphi) * T_m^{\mathbb{D}} \tag{4}$$

where $T_h^{\mathbb{D}}$ is ratio of inter cluster hop devices remaining energy over normal sensor devices which is defined as follows

$$T_h^{\mathbb{D}} = {\vec{L}_{\mathbb{D}}}\Big/{\vec{L}_{\mathbb{S}}} \tag{5}$$

where $|\mathbb{S}|$ and $|\mathbb{D}|$ denote the number of normal sensor devices and inter cluster hop devices respectively, $\vec{L}_{\mathbb{D}}$ is the mean remaining energy of inter cluster hop devices. The device with higher energy is selected as the inter cluster hop device by maximizing $T_h^{\mathbb{D}}$. Similarly the $T_m^{\mathbb{D}}$ can be expressed as follows,

$$T_m^{\mathbb{D}} = {\vec{Z}_{\mathbb{S}}}\Big/{\vec{Z}_{\mathbb{D}}} \tag{6}$$

For selection of cluster head $\mathcal{D}_y$ and its corresponding inter cluster hop device $\mathbb{D}_u$, the location of base station $\mathcal{S}$ and cluster head $\mathcal{D}_y$ is considered. The transmission cost among cluster head and inter cluster hop device can be reduced by maximizing $T_m^{\mathbb{D}}$.

The optimization problem of cluster head selection is solved by applying enhanced ICA. Firstly initialize the optimization problem and parameters, initialize a set of countries and the size of countries is expressed as M, each countries i has a position vector $g_a = [g_{a1}, g_{a2}, g_{a3}, \dots, g_{aj}]$ and velocity vector $w_a = [w_{a1}, w_{a2}, w_{a3}, \dots, w_{ad}]$ is used to specify the current state, where a is a positive param indexing the countries in a colony and j depicts the problem dimension. Secondly we compute the fitness of each country, each country compute its fitness function based on Eq. (1) and Eq. (4). During this phase each country maintains local best solution $R_a = [r_{a1}, r_{a2}, r_{a3}, \dots, l_{lj}]$ by itself and global best solution $R_l = [r_{l1}, r_{l2}, r_{l3}, \dots, l_{aj}]$ achieved by any country in a colony. Then it computes and finds the global and local best position based on which imperialist are added. Thirdly updating position and velocity, in each round there is a change in velocity of each country towards local best and global best positions. The position of countries is updated as follows

$$g_{ab}^{\mathbb{t}+1} = g_{ab}^{\mathbb{t}} + w_{ab}^{\mathbb{t}+1}, \tag{7}$$

The velocity of countries is updated as follows

$$w_{ab}^{\mathbb{t}+1} = \mathbb{v} w_{ab}^{\mathbb{t}} + \mathbb{u}_1 \mathbb{z}_1 (r_{ab}^{\mathbb{t}} - g_{ab}^{\mathbb{t}}) + \mathbb{u}_2 \mathbb{z}_2 (r_{lb}^{\mathbb{t}} - g_{lb}^{\mathbb{t}}) \tag{8}$$

where the notation of g_{ab}, r_{ab} and r_{ab} is similar to w_{ab}. w_{ab} is the bth dimension of ath countries velocity and it is generally limited to closed interval of $[w_{\downarrow}, w_{\uparrow}]$ to prevent colonies from moving beyond the search space boundary conditions. The acceleration param $\mathbb{u}_1$ and $\mathbb{u}_2$ are controlled based on evolutionary states. Coefficient $\mathbb{z}_1$ and $\mathbb{z}_2$ are arbitrarily generated param between zero to one for jth dimension and $\mathbb{v}$ is the inertia weight. The weights $\mathbb{V}$ play a critical part in controlling influence of velocity of a country of present one. This is done to bring tradeoff between global and local search (i.e. large and small inertial weight update respectively). The updation of weight is modified to prevent the proposed optimization model in getting stuck in local optima which is as follows

$$\mathbb{V} = \left(\frac{\mathbb{I}_{\uparrow} - \mathbb{I}_{\mathcal{C}}}{\mathbb{I}_{\uparrow}}\right) * (\mathbb{V}_{\uparrow} - \mathbb{V}_{\downarrow}) + \mathbb{V}_{\downarrow} \tag{9}$$

where $\mathbb{I}_{\uparrow}$ is the maximum amount iteration permitted, $\mathbb{I}_{\mathcal{C}}$ is the present iteration, $\mathbb{V}_{\downarrow}$ is the minimum inertial weight and $\mathbb{V}_{\uparrow}$ is the maximum inertial weight. The present finest solution is chosen after termination statement is met. This is the ideal strategy for optimization is computed.

b) *System model for Symmetric ECC security model for cluster based WSN:*

This section describes the detail of proposed symmetric based ECC model for cluster based routing model for WSN. The sensor network is composed of set of cluster head $\mathcal{D}$, cluster member device K and set of hop device $\mathbb{D}$. The sensor device sense the data and transmit to its cluster head, then the cluster head aggregates the data and transmit it to the hop device towards sink/base station. Further, to provision secure routing design. This work present a secure and efficient security mechanism for WSN using cryptography mechanism. For provisioning superior security mechanism asymmetric cryptography approach such as RSA, ECC etc. is used. However, it incurs higher computation overhead affecting lifetime performance of sensor network. To overcome the research challenges, this work present a symmetric based ECC model to overcome computation overhead issues of WSN. For attaining secure routing design, firstly, a scalable key administration model is presented which is distributed in nature. i.e., the secure key administration is to distribute keys to each cluster head, which is responsible administration and distributing keys among its respective cluster members. Key administration process is composed of key generation, key exchanges, data encryption and data decryption. In secure key administration, mutual session key ($MSKs$) of all hop device-cluster head/ cluster member pairs are pre-constructed, and not established in real-time. The pre-construction process is that, the cluster head/member first register its public key with the hop device toward its sink. Then each hop device-cluster head/member device pair computes their MSK when the hop transmission (inter cluster) device is constructed, based on the cluster head/member's public keys, and utilizes MSK to build a secure hop-cluster head/member channel in the hop based transmission (inter cluster communication).

Similarly, for intra cluster communication, i.e., cluster head-cluster member channel and secure hop-cluster head/members channel are exactly identical except that constructing secure channels in intra cluster transmission is a real-time operation.

This work assume that the member device route the data to the cluster head with maximum connectivity and energy cluster head. From cluster head, it is transmitted through hop device toward sink. Since sensor devices has limited coverage area. Therefore, it is composed of following path from senor device towards sink through cluster head and set of hop devices as

$$Path(\mathcal{K} \to \mathcal{D} \to \mathbb{D}^* \to Sink) \qquad (10)$$

Firstly, let's consider the following $Path(\mathcal{K} \to \mathcal{D} \to Sink)$. Under this assumption, firstly, the cluster member $\mathcal{K}$ and cluster head $\mathcal{D}$ generates an MSK' in real time. Secondly, the cluster member encrypt packet with MSK', and transmits the cipher content to the cluster head. Thirdly, the cluster head decrypt the obtained cipher content with MSK'. Fourthly, the cluster head and the sink have a pre-constructed MSK''. Then, the cluster head encrypt data with MSK'', and sends cipher content to the sink. The sink decrypt the received cipher content with the MSK''. Secondly, let's consider the following $Path(\mathcal{K} \to \mathcal{D} \to \mathbb{D}^* \to Sink)$. Under this assumption, firstly, the cluster member and cluster head generate a MSK'. Secondly, the cluster member encrypts data with MSK', and transmit the cipher content to the cluster head. Thirdly, the cluster head decrypts the obtained cipher content with the MSK'. Fourthly, cluster head and sink have pre-constructed MSK''. Further, the cluster head encrypt the data with MSK'', and transmit the cipher content to the hop device. Then, the hop device simply forward this cipher content to the sink device. Lastly, the sink decrypts the obtained cipher content with the MSK''. Overall, the cluster member only construct secure channels among cluster head, and never perform direct communication with sink. The cluster head is always considered to be the last cluster/hop device toward sink with secure channels.

c) Symmetric ECC security model for cluster based routing model for WSN:

This section present a secure and efficient symmetric ECC (SESECC) security model for WSN. The SECC is designed considering cluster based WSN. SESECC is composed of cluster head that manages secure session among its member and the hop device. Further, SESECC is designed using self-certified public key model [32], [33] which composed of following features. Firstly, the secret key among cluster member can be established together by cluster head and the cluster member and cluster head has no information about it. Secondly, a cluster member can authenticate the validness of self-certified public key given by a cluster head by using its own secret key. As a result, no added certificate is needed. Thirdly, the job of public key correctness can be achieved using key distribution in a logical manner. Therefore, it aid in enhancing system efficiency and reducing computational cost as compared with state-of-art certificate based methods.

The symmetric ECC (SECC) is composed of following stages such as Sensor Device Setup Stage (SDSS) and Secure Communication stage (SCS). The SECC is designed considering following setups. Firstly, the field size q is generally a power of two or an odd prime, and its size is around 160 bits. Secondly, an elliptic curve F over G_q is $F: b^2 = a^3 + xa + y$, where the two field elements $x, y \in G_q$, and $4x^3 + 27y^2(modq) \neq 0$; and all the points $(a, b), a \in G_q, b \in G_q$, on F from the set of $F(G_q)$ composed of a point P represted as the point at infinity. In the process z, H depicts elliptic curve (EC) parameter for token, session keys, public keys parameter, "." depicts multiplication of EC, where $z \in [2, o-2]$, an arbitrary integer parameter, and $H \in F(G_q)$. z depicts most integers in SECC, such as identities, arbitrary number, private and master keys. Further, Y is a base point of order o over $F(G_q)$, where o is a larger prime of 160 bits, and the amount of G_q rational points on F depicted by $\#F(G_q)$, is divisible by o. Then, $A(H)$ is the outcome of points $H's$ x-cordinates, where H is an EC point order o over $F(G_q)$. Further, $i(.)$ is a unidirectional hash operation that allows a parameter size input and builds a fixed size outcome parameter k, where $k \in [2, o-2]$ and its size is equal to 160 bits. Lastly, $t(J, l)$ is a symmetric block cipher methodology operation by utilizing a symmetric key l. If the input J is a plain data, then the outcome is the cipher data. If J is a cipher data, then the outcome is back to its original plain data.

$\mathbb{M}_{\mathcal{K}}$	Master key
$\mathbb{I}_{\mathcal{K}}$	Identity key
$\mathbb{P}_{\mathcal{K}}$	Public key (Session validation)
$\mathbb{S}_{\mathcal{K}}$	Private keys
$\mathbb{R}_{\mathcal{K}}$	Request tickets
$\mathbb{O}\mathbb{T}_{\mathcal{D}}$	Observer tickets
$\mathbb{S}\mathbb{T}_{\mathcal{K}}$	Session tickets
$\mathbb{S}\mathbb{P}_{\mathcal{K}}$	Specific session
$\mathbb{C}\mathbb{T}_{\mathcal{K}}$	Communication tickets

d) Sensor Device Setup Stage:

The SDSS packet routing is modelled as follows. Firstly, the cluster member possess its master key $\mathbb{M}_{\mathcal{K}} \in [2, o-2]$ and identity $\mathbb{I}_{\mathcal{K}} \in [2, o-2]$, and utilizes these to construct $\mathbb{R}_{\mathcal{K}}$ (request tickets) and Y (random hashing).

$$\mathbb{R}_{\mathcal{K}} = i(\mathbb{M}_{\mathcal{K}} \| \mathbb{I}_{\mathcal{K}}).Y. \tag{11}$$

Then, the cluster member transmits a S_{req} which composed of $\mathbb{I}_{\mathcal{K}}$ and $\mathbb{R}_{\mathcal{K}}$ to the cluster head. Secondly, the cluster head evaluates $\mathbb{P}_{\mathcal{K}}$, along with session based initialization arbitrary number $\mathbb{A}_{\mathcal{D}} \in [2, o-2]$ as follows

$$\mathbb{P}_{\mathcal{K}} = \mathbb{R}_{\mathcal{K}} + \left(\mathbb{A}_{\mathcal{D}} - i(\mathbb{I}_{\mathcal{K}})\right).Y. \tag{12}$$

The cluster head builds an observer ticket $\mathbb{OT}_{\mathcal{D}}$ for the cluster member with it's $\mathbb{S}_{\mathcal{D}}$ as follows

$$\mathbb{OT}_{\mathcal{D}} = \mathbb{A}_{\mathcal{D}} + \mathbb{S}_{\mathcal{D}}\left(A(\mathbb{P}_{\mathcal{K}}) + i(\mathbb{I}_{\mathcal{K}})\right) (\text{mod } o). \tag{13}$$

Then, the cluster head responses the S_{resp} possessing $\mathbb{P}_{\mathcal{K}}$ and $\mathbb{OT}_{\mathcal{D}}$ for arising the $\mathbb{S}_{\mathcal{K}}$ at the cluster member. Lastly, the cluster member expresses the respective private key $\mathbb{S}_{\mathcal{K}}$ as follows

$$\begin{aligned}\mathbb{S}_{\mathcal{K}}.Y = \mathbb{P}_{\mathcal{K}} + i(\mathbb{I}_{\mathcal{K}}).Y \\ + \Big[\big(Y(\mathbb{P}_{\mathcal{K}}) \\ + i(\mathbb{I}_{\mathcal{K}})\big)(\text{mod } o)\Big].\mathbb{P}_{\mathcal{D}}\end{aligned} \tag{14}$$

The Eq. (14), shows that the cluster head can give the $\mathbb{P}_{\mathcal{K}}$ without knowing the $\mathbb{S}_{\mathcal{K}}$ and the $\mathbb{M}_{\mathcal{K}}$, so the cluster head behaves as a zero knowledge proof. Therefore, only the cluster member can possess the $\mathbb{S}_{\mathcal{K}}$ and the $\mathbb{M}_{\mathcal{K}}$. As a result, the cluster head can manage large number of cluster members in a dynamic manner. Since the cluster head is not in charge of storing secret information of the cluster members.

e) Secure communication stage:

Post completion of SDSS, the SCS is initialized which is modelled as follows. Firstly, the cluster member constructs a session ticket $\mathbb{ST}_{\mathcal{K}}$ with a time specific session arbitrary parameter $\mathbb{SP}_{\mathcal{K}} \in [2, o-2]$ as follows

$$\mathbb{ST}_{\mathcal{K}} = \mathbb{SP}_{\mathcal{K}}.Y(\text{mod } o). \tag{15}$$

Then, the cluster member transmits a C_{req} possessing the $\mathbb{I}_{\mathcal{K}}$ and the $\mathbb{ST}_{\mathcal{K}}$ to the cluster head. Secondly, post obtaining C_{req}, the cluster head obtains the $\mathbb{P}_{\mathcal{K}}$ in its public keys sets. Then, the cluster head constructs its session ticket $\mathbb{ST}_{\mathcal{D}}$ with time specific session arbitrary parameter $\mathbb{SP}_{\mathcal{D}} \in [2, o-2]$ as follows

$$\mathbb{ST}_{\mathcal{D}} = \mathbb{SP}_{\mathcal{D}}.Y(\text{mod } o). \tag{16}$$

The cluster head transmit it again a C_{resp} possessing the $\mathbb{I}_{\mathcal{D}}$, $\mathbb{ST}_{\mathcal{D}}$, and $\mathbb{P}_{\mathcal{D}}$ to make sure that the cluster member computes the mutual session key MSK. Further, the cluster head computes the MSK with its communication ticket $\mathbb{CT}_{\mathcal{D}}$ as follows

$$\begin{aligned}MSK = \mathbb{SP}_{\mathcal{D}}.\mathbb{CT}_{\mathcal{D}} + \mathbb{S}_{\mathcal{D}}.\mathbb{ST}_{\mathcal{K}} \\ = (\mathbb{SP}_{\mathcal{D}}.\mathbb{S}_{\mathcal{D}} \text{ mod } o).Y + (\mathbb{S}_{\mathcal{D}}.\mathbb{SP}_{\mathcal{D}} \text{ mod } o).Y\end{aligned} \tag{17}$$

where $\mathbb{CT}_{\mathcal{D}}$ can be computed as follows

$$\begin{aligned}\mathbb{CT}_{\mathcal{D}} = \mathbb{P}_{\mathcal{K}} + i(\mathbb{I}_{\mathcal{K}}).Y \\ + \Big[\big(A(\mathbb{P}_{\mathcal{K}}) \\ + i(\mathbb{I}_{\mathcal{K}})\big)\text{mod } o\Big].\mathbb{P}_{\mathcal{D}}\end{aligned} \tag{18}$$

Then, the cluster member computes MSK using information of C_{resp} with its communication tickets $\mathbb{CT}_{\mathcal{K}}$ as follows

$$\begin{aligned}MSK = \mathbb{SP}_{\mathcal{K}}.\mathbb{CT}_{\mathcal{K}}.\mathbb{ST}_{\mathcal{D}} \\ = (\mathbb{SP}_{\mathcal{K}}.\mathbb{S}_{\mathcal{D}} \text{ mod } o).Y + (\mathbb{S}_{\mathcal{K}}.\mathbb{SP}_{\mathcal{D}} \text{ mod } o).Y\end{aligned} \tag{19}$$

where $\mathbb{CT}_{\mathcal{K}}$ can be computed as follows

$$\begin{aligned}\mathbb{CT}_{\mathcal{K}} = \mathbb{P}_{\mathcal{D}} + i(\mathbb{I}_{\mathcal{D}}).Y \\ + \Big[\big(A(\mathbb{P}_{\mathcal{D}}) \\ + i(\mathbb{I}_{\mathcal{D}})\big) \text{ mod } o\Big].\mathbb{P}_{\mathcal{D}}\end{aligned} \tag{20}$$

Using Eq. (17), and (Eq. (19), the cluster head and the cluster member can mutually use same MSK, so a secure communication is administered. Then, the cluster member initialize to transmit data N secured by the MSK as follows

$$D = t(N, MSK). \tag{21}$$

Then, the cluster head can obtain N by using following expression

$$N = t(D, MSK). \tag{22}$$

The secure communication will be terminated when session ticket completes. Post completion of secure communication termination, the cluster member should restart a new session using methods defined in SECC. Experiment are conducted to evaluate performance of proposed SESECC for cluster based WSN over state-of-art model in next section. The usage of SEECC aided in reducing communication overhead, and enhance the lifetime of WSN which is experimentally proved in next section below.

III. SIMULATION RESULT AND ANNALYSIS

The system environment used is windows 10 enterprises operating system, 64-bit Quad core processor, 2GB NVDIA CUDA Dedicated Graphic card, with 16GB of RAM. We have used sensoria simulator [34] which is designed using dot net framework 4.0 and C# as a programming language. We have conducted simulation study to evaluate communication overhead, and packet transmission delay performance and compared our SESECC over SEECC. Further, experiment are conducted to evaluate network lifetime performance of SESECC over EEHC-ECC. And LEACH. The simulation parameter used for experimental analysis is shown in table 1 below.

TABLE I. SIMULATION PARAMETER CONSIDERED

Network Parameter	Value
Network Size	50m * 50m
Number of sensor devices	400, 500, 600, 700, 800, 1200, & 1600
Number of Base station	1
Initial energy of sensor nodes	0.2 J
Radio energy dissipation	50 nj/bit
Data packets length	2000 bits
Transmission speed	200 bit/s
Bandwidth	10000 bit/s
Idle energy consumption (Eelec)	50 nj/bit
Data packet processing delay	0.1 ms
Amplification energy (Emp)	100 pJ/bit/m2

a) Communication overhead performance:

This section evaluated performance evaluation of communication overhead incurred by SESECC (symmetric ECC) over SEECC (Asymmetric ECC). The communication overhead is computed as an energy induced in transmitting packets in control channel for attaining secure communication among sensor device toward sink. The communication overhead incurred by SESECC over SEECC considering varied sensor device is graphically shown in Fig.

2. The outcome shows SESECC reduces communication overhead by 22.001%, 26.16%, 25.87%, and 38.71% over SEECC considering 400, 800, 1200, and 1600 sensor device, respectively. From figure it can be seen the communication overhead increases with increase in sensor device for both protocols and linearly sharply for SEECC. This is due to as node is increased, the member size of cluster also increases. An average communication overhead reduction of 28.18% is attained by SESECC over SEECC considering varied sensor device. From, result SESECC attained significant performance when compared with exiting model [27].

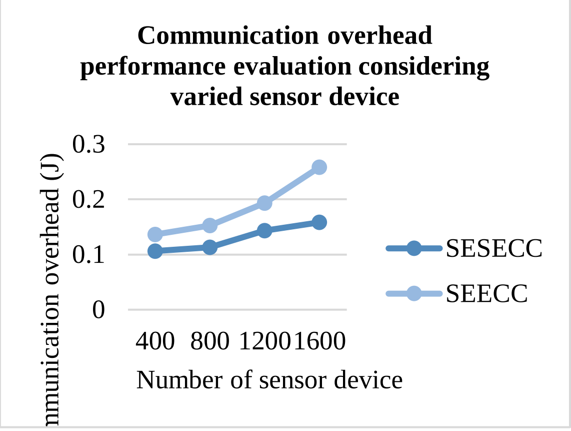

Fig. 2. Communication overhead performance evaluation for varied sensor device

b) Packet processing time performance evaluation for varied sensor device:

This section evaluated performance evaluation of packet processing time incurred by SESECC (symmetric ECC) over SEECC (Asymmetric ECC). The packet processing time is computed as a time taken to securely transmit data from source to destination which composed of phases such key generation, session management for secure communication, encrypting and decrypting. The packet processing time taken by SESECC over SEECC considering varied sensor device is graphically shown in Fig. 3. The outcome shows SESECC reduces packet processing time by 7.89%, 12.04%, 13.53%, and 16.87% over SEECC considering 400, 800, 1200, and 1600 sensor device, respectively. From figure it can be seen the packet processing time increases with increase in sensor device for both protocols and linearly sharply for SEECC. This is due to as node is increased, the member size of cluster also increases. An average packet processing time reduction of 12.58% is attained by SESECC over SEECC considering varied sensor device. Further, experiment are conducted to evaluate running time. The existing model [26] attained an average running time of 9 milliseconds and proposed SESECC attained an average running time of 2.14 milliseconds. The overall result attained shows efficiency of SESECC model.

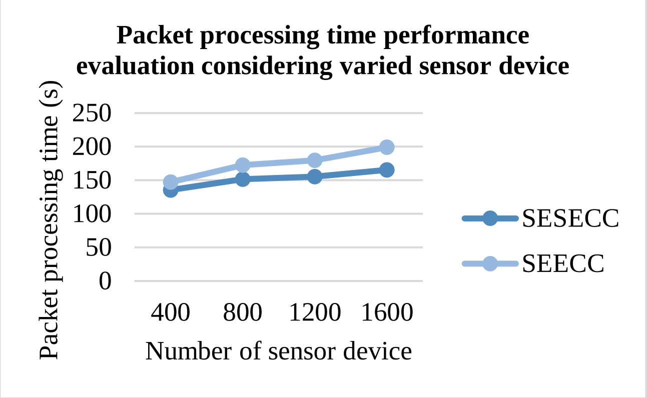

Fig. 3. Packet processing time performance evaluation for varied sensor device

c) Lifetime performance evaluation considering varied sensor device:

This section evaluated performance evaluation of lifetime attained by SESECC (Asymmetric ECC) model over EEHC-ECC (Symmetric ECC) [35]. The lifetime performance attained by SESECC over EEHC-ECC considering varied sensor device is graphically shown in Fig. 3. The outcome shows SESECC improves lifetime performance by 76.59%, 86.32%, and 85.42% over LEACH considering 500, 600, and 700 sensor device, respectively. Similarly, SESECC improves lifetime performance by 68.69%, 74.27%, and 68.41%over EEHC-ECC considering 500, 600, and 700 sensor device, respectively. An average lifetime improvement of 70.45%, and 82.77% is attained by SESECC over LEACH and EEHC-ECC, respectively considering varied sensor device. The overall result attained shows lifetime efficiency of proposed SESECC model.

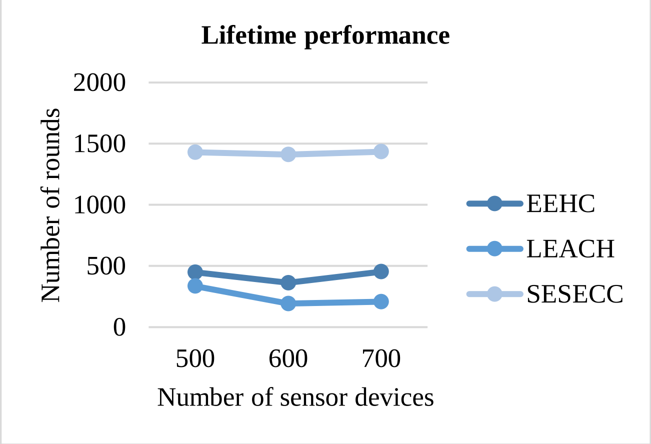

Fig. 4. Lifetime performance evaluation for varied sensor device

IV. Conclusion

Clustering technique play an important factor in enhancing the lifetime of sensor network. However, improper cluster selection technique will lead to performance degradation. For better cluster selection evolutionary computing is adopted by existing approaches.

However, they suffers NP-Hardness problem and connectivity issues is neglected. To overcome research challenges, this work presented Multi-objective imperialist competitive algorithm for cluster head selection. Further, the WSN suffer from number of security issues which requires to bring a god tradeoff between secure and energy efficacy. For attaining secure and energy efficient communication, this work presented a novel symmetric ECC. The SESECC model reduces communication overhead among cluster head and can accommodate more cluster member. Since it does not possess or store any key information of its member. Further, it preserve privacy of data and its user. From result obtained it can be seen the SESECC model reduces communication overhead by 28.18%, reduces packet processing time12.58%, over SEECC. Further, improves lifetime performance by 70.45%, and 82.77% over LEACH and EEHC-ECC. The overall result attained by SESECC shows robust and scalable performance. Future work this work would consider performance evaluation over exiting model considering first sensor node death, loss of connectivity etc. Further, would consider incorporating SECC for EEHC protocol and evaluated its performance.

REFERENCES

1. I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, Aug 2002.
2. Y. Wang, G. Attebury, and B. Ramamurthy, “A survey of security issues in wireless sensor networks,” IEEE Communications Surveys Tutorials, vol. 8, no. 2, pp. 2–23, Second 2006.
3. L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in Proc. of ACM CCS, pp. 41–47, 2002.
4. H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in Proc. of IEEE S&P, pp. 197–213, 2003.
5. K. N. SunilKumar and Shivashankar, " Security Issues in Wireless Sensor Network – A Review," https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7784988, 2016.
6. K. N. SunilKumar and Shivashankar, "A review on security and privacy issues in wireless sensor networks," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, 2017, pp. 1979-1984, 2017.
7. T. M. Rahayu, S. Lee and H. Lee, "Survey on LEACH-based security protocols," 16th International Conference on Advanced Communication Technology, Pyeongchang, pp. 304-309, 2014.
8. S. Cirani and M. Picone, ``Wearable computing for the Internet of Things," IT Prof., vol. 17, no. 5, pp. 35-41, Sep. 2015.
9. A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, ``Internet of Things for smart cities," IEEE Internet Things J., vol. 1, no. 1, pp. 22-32, Feb. 2014.
10. M. Simsek, A. Aijaz, M. Dohler, and J. Sachs, ``5G-enabled tactile Internet," IEEE J. Sel. Areas Commun., vol. 34, no. 3, pp. 460-473, Mar. 2016.
11. J. Fan, F. Han, and H. Liu, ``Challenges of big data analysis," Nat. Sci. Rev., vol. 1, no. 2, pp. 293-314, 2014.
12. O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow and M. N. Hindia, "An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges," in IEEE Internet of Things Journal.doi: 10.1109/JIOT.2018.2844296, 2018.
13. . Qiu, N. Chen, K. Li, M. Atiquzzaman and W. Zhao, "How Can Heterogeneous Internet of Things Build Our Future: A Survey," in IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2011-2027, thirdquarter 2018. doi: 10.1109/COMST.2018.2803740, 2018.
14. E. Sisinni, A. Saifullah, S. Han, U. Jennehag and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," in IEEE Transactions on Industrial Informatics. doi: 10.1109/TII.2018.2852491, 2018.
15. P. Nayak and A. Devulapalli, "A Fuzzy Logic-Based Clustering Algorithm for WSN to Extend the Network Lifetime," in IEEE Sensors Journal, vol. 16, no. 1, pp. 137-144, Jan.1, 2016.
16. P. Nayak and B. Vathasavai, "Energy Efficient Clustering Algorithm for Multi-Hop Wireless Sensor Network Using Type-2 Fuzzy Logic," in IEEE Sensors Journal, vol. 17, no. 14, pp. 4492-4499, July15, 15 2017.
17. S. Rani; S. H. Ahmed; R. Talwar; J. Malhotra, "Can Sensors Collect Big Data? An Energy Efficient Big Data Gathering Algorithm for WSN," in IEEE Transactions on Industrial Informatics , vol.PP, no.99, pp.1-1, 2017.
18. H. K. Deva Sarma, R. Mall and A. Kar, "E2R2: Energy-Efficient and Reliable Routing for Mobile Wireless Sensor Networks," in IEEE Systems Journal, vol. 10, no. 2, pp. 604-616, June 2016.
19. C. W. Tsai, T. P. Hong and G. N. Shiu, "Metaheuristics for the Lifetime of WSN: A Review," in IEEE Sensors Journal, vol. 16, no. 9, pp. 2812-2831, May1, 2016.
20. M. Parsapoor and U. Bilstrup, "An Imperialist Competitive Algorithm for Interference-Aware Cluster-Heads Selection in Ad Hoc Networks," 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, Victoria, BC, 2014, pp. 41-48.
21. C. H. Chen and W. H. Chen, "United-Based Imperialist Competitive Algorithm for Compensatory Neural Fuzzy Systems," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 46, no. 9, pp. 1180-1189, Sept. 2016.
22. D. S. Weile and E. Michielssen, “Genetic algorithm optimization applied to electromagnetics: A review,” IEEE Trans. Antennas Propag., vol. 45, no. 3, pp. 343–353, 1997.
23. J. Prasad and T. Souradeep, “Cosmological parameter estimation using particle swarm optimization (PSO),” Phys. Rev. D, vol. 85, no. 12, Art. ID 123008, 2012.
24. C. Laoudias, A. Moreira, S. Kim, S. Lee, L. Wirola and C. Fischione, "A Survey of Enabling Technologies for Network Localization, Tracking, and Navigation," in IEEE Communications Surveys & Tutorials. doi: 10.1109/COMST.2018.2855063.
25. R. Eletreby and O. Yagan, "Connectivity of Wireless Sensor Networks Secured by Heterogeneous Key Predistribution Under an On/Off Channel Model," in IEEE Transactions on Control of Network Systems. doi: 10.1109/TCNS.2018.2808141, 2018.
26. P. Ting, J. Tsai and T. Wu, "Signcryption Method Suitable for Low-Power IoT Devices in a Wireless Sensor Network," in IEEE Systems Journal, vol. 12, no. 3, pp. 2385-2394, 2018.
27. M. Rahman and K. El-Khatib, "Secure Time Synchronization for Wireless Sensor Networks Based on Bilinear Pairing Functions," in IEEE Transactions on Parallel and Distributed Systems. doi: 10.1109/TPDS.2010.94, 2018.
28. L. B. Oliveira, R. Dahab, “Pairing-Based Cryptography for Sensor Networks,” 5th IEEE International Symposium on Network Computing and Applications (NCA’06), Cambridge/MA, USA (fast abstract), July 2006.
29. W. Du, R. Wang, and P. Ning, “An efficient scheme for authenticating public keys in sensor networks,” Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, Urbana-Champaign, IL, USA, pp. 58-67, 2005.
30. Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig,and Eric Wustrow, “Elliptic Curve Cryptography in Practice” 2014.
31. Elaine Brow “Elliptic Curve Cryptography”, 2010.
32. D. He, S. Zeadally, N. Kumar and W. Wu, "Efficient and Anonymous Mobile User Authentication Protocol Using Self-Certified Public Key Cryptography for Multi-Server Architectures," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 2052-2064, Sept. 2016.
33. S. Gupta, A. Kumar and N. Kumar, "Design of ECC based authenticated group key agreement protocol using self-certified public keys," 2018 4th International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, pp. 1-5 2018.
34. J. N. Al-Karaki and G. A. Al-Mashaqbeh, "SENSORIA: A New Simulation Platform for Wireless Sensor Networks," 2007 International Conference on Sensor Technologies and Applications (SENSORCOMM 2007), Valencia, 2007, pp. 424-429.
35. H. V. Chaitra and G. K. Ravikumar, "A secure and energy efficient cluster optimization by using hierarchial clustering technique," 2016 3rd International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, pp. 93-97, 2016.