International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/207983 Volume 8, Issue 1, January – February (2021)

RESEARCH ARTICLE

Elliptic Curve Cryptography based Secure Image Transmission in Clustered Wireless Sensor Networks

Rekha
Department of Computer Science and Applications, Maharishi Markandeshwar (Deemed to be University), Mullana (Ambala), India.
rekha_dalia@yahoo.com

Rajeev Gupta
Department of Computer Science and Engineering, Maharishi Markandeshwar (Deemed to be University), Mullana (Ambala), India.
rajeev.gupta@mmumullana.org

Received: 20 December 2020 / Revised: 25 January 2021 / Accepted: 19 February 2021 / Published: 23 February 2021

Abstract – Wireless Sensor Networks (WSN) is arising as a potential computing platform in diverse zones such as weather forecasting, modern robotization, medical health care, and military systems, etc. Since the sensors are constantly gathering information from the actual world and communicate with one another through remote connections, keeping up the security and protection of WSN communication is a prerequisite. In this paper, safe confirmation and key organization scheme dependent on Elliptic Curve Cryptography (ECC) has been suggested to make sure about information/picture transmission in WSNs. The scheme proposed in this paper is protected, competent, and appropriate for providing sensor technology based IoT services and applications. The protocol provides all the security features such as mutual authentication, confidentiality, data integrity, perfect forward secrecy, fair key agreement, etc. and is secure against hello flood attack, DoS attack, man-in-middle attack, etc. Simulation software AVISPA has confirmed the safety of the protocol for the known assaults. The performance analysis ensures the superiority of the projected proposal over the existing schemes.

Index Terms – WSN, Security, Elliptical Curve Cryptography (ECC), Automated Validation of Internet Security Protocols and Applications (AVISPA).

1. INTRODUCTION

In recent times, WSN is becoming popular due to its versatility in providing services for monitoring activities of surrounding environments, use in an extensive range of applications, and ease of deployment. Wireless links are established between the sensor nodes which are dissipated over a specific region[1]. Sensor nodes have the capability to process, sense, aggregate, and broadcast the information to a federal node called base station or sink node. These nodes have a battery that cannot be easily recharged which ultimately reduces the lifetime of the sensor node and WSN as well[2,3]. Another challenging aspect of WSN is energy efficiency. To overcome this challenge, sensor nodes are arranged in zones called clusters, and a special node called Cluster head(CH) is elected depending upon its energy utilization to broadcast the information to the sink node[4,5].

With the evolution of smart computing devices and wireless communication, visual communication is overpowering the textual communication mechanisms. A large amount of data can be transferred easily through images as compared to textual information[6,7]. Many real-time applications prefer embedded sensors that may have additional components such as a camera for capturing images or videos, a microphone to record audio, mobilize to change its location, and GPS to find its location. After incorporating all these features, new dimensions like vineyard monitoring, law enforcement, traffic monitoring, health monitoring, target tracking in military areas, etc. are discovered for applicability of WSN[8,9]. So, CH can easily transfer these images to the base station. Increased usage of WSN, the security of images transferred along with energy efficiency turn out to be a necessary aspect to be considered in WSN.

Consequently, while transferring the video and image, security is a significant and challenging matter to be considered. Disregarding the way that there is a lot of secure pictures preparing plans expected for picture communication over a WSN, the constrained resources make it insubstantial to be used in this area[10,11]. Moreover, the recent protected information communication patterns are focused on the content information and cannot be used in application of image transmission. Besides, protected picture transmission is a major issue in this area particularly for the application that utilizes image as its fundamental information, for example, military applications[12,13]. As intruders can launch both passive and active attacks on the images being transferred, so

RESEARCH ARTICLE

security should be provided either before or during the transmission of data.

To evade asset utilization in WSN, like, energy utilization while image broadcast, numerous specialists have coordinated and proposed picture encryption and transmission strategies. In any case, the storage capacity required for keeping the encryption key in these techniques despite everything speaks to an interesting issue for scientists.

Lightweight cryptography is one of the astounding areas of research in security. It has been proposed for the areas where highly constrained devices are interconnected by wireless communication and work for the particular application. Existing cryptography algorithms do not fit into constrained devices[14].ECC provides high cryptographic strength similar to the symmetric schemes like the RSA, but the key size is very small. Due to the smaller key size, ECC comes out to be an ideal option for an area like WSN which has devices with limited resources like battery, memory, and processing capabilities[15].

1.1. Research Motivation and Objectives

To resolve the excessive asset utilization in WSN such as energy during image broadcast, several image encryption and transmission schemes have been proposed over the years. However, in these algorithms memory required for the storage of the generated encryption key is large and hence still an upcoming topic for researchers. Using elliptic curve cryptography and a key agreement protocol, an authentication scheme is proposed in this paper. Using this protocol, the sensor nodes mutually produce a symmetric session key which can be used to encrypt the image and transmit it over the insecure channel to the receiving node. The receiving node will use its own independently generated session key to decrypt the encrypted image. ECC offers high cryptographic strength similar to the symmetric schemes as the RSA because of smaller size of key. For example, both ECC based 256-bit key and RSA key of size 3072-bit provide the same level of security. That's why ECC gets the more priority related to the security of devices which have low storage capacity or limited data processing resources, e.g.in the field of WSN.

1.2. Paper Organization

The paper is coordinated into various segments: Section 2 portrays the writing survey. ECC based authentication and key generation procedure are proposed in Segment 3. Informal security study of the planned procedure is discussed in part 4. Segment 5 presents the performance analysis of the investigated protocol as compared to existing protocols. Section 6 covers the simulation detail, which is followed by segment 7 that covers the conclusion part of the paper.

2. LITERATURE REVIEW

Due to the high usage of WSN in various areas like military, civil, hospitals, etc. both the industry and academia researchers have been engrossed in this area. In this section literature study of existing secure image transmission methods in WSN and the proposed method to transmit the secure image is done.

Extensive use of WSNs in many application areas like military, indoor climate control, health monitoring, security, industrial applications, environmental sensing, landslide detection, water quality monitoring, and many more compelled the researchers to increase their research in this field. Due to sensitive data transmission in these applications factors like authenticity, integrity and confidentiality should be ensured[16]. To achieve secure data transmission an appropriate authentication protocol is a very challenging aspect to be considered. There are many researchers who have addressed the area of secure data transmission in WSN using cluster head, but, only few researchers raised the issue of secure image transmission using cluster head in WSN. In the current scenario when image transmission is overpowering the textual data, there is an extreme requirement of the study of the security of images transmitted through WSN.

To procure the security in WSN during image transmission, either encryption key should be managed or data access needs to be controlled. To overcome the various security threats, diverse encryption key management schemes like novel hash-based authentication,2-hop multipath, q-composite, and random pairwise schemes have been proposed in[17]–[19] at the cost of large scale attack and compromise of network size. Also, these schemes lead to higher configuration efforts before deployment and large energy consumption due to higher traffic. TinyPK system demonstrated in [20]authentication between node and third party and an individual speck cannot be used to pretend the motes with different identification.

Mykeletin et al. In [2006][21] have given EC-OU in WSN's to accomplish data concealment which increases rises the communication overhead. Olivia et al.[2007]Sec Leach[22]and Wu et al.[2008][23] have used symmetric key methods of cryptography for security but SLEACH algorithm decreased the network performance. Both the key methods prove to be energy efficient and keep the transmitted data safe.

Zhang et al.[2008][23] hashed a generated symmetric key using ESODR algorithm as the hash function. However, the size of the key microscopes, when combined with image transmission. EDRLEACH [24] one of many SLEACH dependent methods. It supplies an efficient way to bypass energy usage whereas ORLEACH [25]increases the time limit &ratio of used energy.

RESEARCH ARTICLE

Biswas and Muthukumarswami[2014][26]proposed an encryption technique that is based on a Chaotic map and ECC. Chatterji et al.[2015][10] have proposed attribute-based encryption using elliptic curve cryptography. Labeled ciphertext with attributes and the user's secret keys have been utilized. The proposed method has been proved to be better than the existing schemes.

Jiang et al. [2016][27] proposed an ECC based authentication scheme that follows the idea of sequential credential in WSNs. The scheme meets the common verification and able to defend against many attacks as compared to He.et.al.[2014] [28].

Homomorphic encryption and ECC are used by Elhoseny[2017][29]for the security of data. Cluster formation happens in virtue of GASONeC algorithm.ECC produces a 176-bit key, distance from CH, and node identification number. The proposed method is valid for text as well as image data.

Inter-cluster multiple key distribution key(ICMDS) is proposed in mehmood[2016][13] to maintain the authenticity of sensor nodes. Two-phase security is suggested. The recovery mechanism helps to save the CH

Authors Harbi et al.[2018] [14]try to improve the communication security in WSN by proposing a safe information broadcast ECC based scheme that produces key of very small size. The recommended protocol can successfully defend against attacks like replay attacks, brute force attacks, sinkhole attacks, and proves to be more secure when compared to existing.

Authors Elhosney et al.[2019][30] encrypts the image by Light Weight Ciphers(LWC). The proposed security model helps in optimal key selection. Also while encrypting, the proposed algorithm by Elhosney et al. takes minimum time to generate the key for decryption of image and prove to be better in term of security accuracy of input images like Horse, Baboon, Barbara, Lena as compared to existing algorithms.

Sumalatha and Nandalal [2020][31] proposed a fuzzy based cross-layer security technique for identifying nasty nodes which hinder the packet movement. Enhanced Convolutionary Neural Network(ECNN) helps in the implementation of false monitoring.

To provide security in WSNs, Jayanthi Ramasamy[2020][1] preferred the Elliptic Curve hill Cipher algorithm. Key's permutation helps in improving their size that is required for the selection of image matrix size. Authors successfully achieved more security, reduced setback, and enhancement in packet release proportion due to a new framework using clusters and ECC algorithm and cluster-based encrypting routing algorithm.

Authors Chi-tung in[2020][32] proposes a distant user validation scheme based upon active ID and temporal credentials for WSNs. For validation of scheme, authors preferred Burrows-Abadi-Needham(BAN) logic. Suggested schemes prove to be better in terms of low energy consumption for authentication, low computational cost. Table 1 covers the limitations of the earlier work.

Authors	Limitations
Chatterjee et al.[10]	Lacks in privacy preservation and prone to cluster head attack
Benenson et al.[33]	Issue of cluster head attack, manage insertion attack, Man-in-middle attack
Yeh et al.[34]	Mutual authentication, Privacy preservation, and insertion attack
Kumar et al.[35]	Lacks in mutual authentication
Das et al.[36]	Man in the middle attack, Insertion attack, Mutual authentication
Lee et al.[32]	Stolen card attack , impersonation, Masquerade attack, and replay
Mishra et al.[37]	privileged insider attack, Denial of service attacks, password change phase, offline password guessing was dependent on the server
Khan et al.[38]	Forward security, Lacks user anonymity, de-synchronization attack, impersonation attack

Table 1 Summary Table of Previous Work

RESEARCH ARTICLE

3. PROPOSED ECC BASED KEY GENERATION PROTOCOL

In the assumed WSN, a total 'm' clusters are formed from 'n' sensor nodes. In every cluster, there exist 'a' number of sensor nodes which comprise of member nodes as well as Cluster Head (CH) node. Presumptions are made that after the deployment, sensor nodes become static. Sensor nodes are capable of communication with each other as well as with cluster head. The CH can speak with one another straightforwardly and hand-off information between its group individuals and the Base Station (BS) which acts as a gateway to some other network.

Two keys master key and an exceptional key are preloaded into nodes which are used for communication with CH and with BS respectively.

One-way Base station loads keyed hash function to all nodes. Nodes maintain a pairwise secret key list. Elliptic curve discrete logarithm help to maintain the safety of the secret key by not transmitting via a network. Only node tampering can be used to compromise it. It is assumed that after deployment, the network remains secure for 't' time an intruder can attack after these t units of time. Keys are updated regularly after every session and a table is maintained for updated keys.

3.1. Clustering Processes

In the proposed work, equal-sized zones are formed in the network, and then, a suitable cluster head is elected from each zone using ANP (Analytical Network protocol) method as explained in **Error! Reference source not found.**. Connectivity based clustering model is being used which considers the distance, energy of the cluster head, and its distance from the BS.

Criteria like Distance of nodes from CH (DNCH), Residual Energy(RE), Energy Consumption Rate(ECR), Initial Energy(IE), Average Energy of Network(AEN) have been finalized for the cluster head selection from a single zone [39].

To maintain and update the cluster three processes are followed. The process of joining and leaving a cluster is very basic and is described below.

3.1.1. To Join a Cluster

As the nodes have the awareness about the identity of each cluster and its boundaries, each node transmits a HELLO message while inflowing a new cluster. If the cluster head sends the acknowledgment, then that particular node may become the cluster member. Otherwise, the node will appeal to the server for a new process of cluster head election.

3.1.2. To Leave a Cluster

Cluster member/node can leave a cluster without explicitly notifying the cluster head or server. A node can be removed from a cluster if: no beacons are arriving from it within a stipulated period, neither the server nor CH receives a beacon from it and the node is out of the cluster boundary.

3.1.3. Cluster Head (CH) Selection

Using certain metrics, the server associated with the cluster can select the cluster head. The server executes the CH election algorithm and after CH selection notifies it of its status. Elected node after selection starts performing as the CH until there is some change in the topology. Reselection of CH is done as per the request of the server or under some dynamic changes prevailing under the environment.

3.2. Assumptions

In the proposed work, an appropriate model has been considered for these sensor networks. It depends upon comparable models utilized in [4, 21]. Assumptions made for the future network shown below:

- Homogeneous sensor nodes are haphazardly distributed and every node has a unique ID.
- The nodes share their knowledge with the CH at periodic intervals.
- Each node can collect information and compress the data packets into one packet before sending.
- It is assumed that the BS has a constant power supply and so, has no energy constraints.
- Nodes have awareness about location, i.e. they have GPS capability.
- Channel being used is bidirectional for the entire network.
- Initially, the CH is selected using the proposed algorithm 1 but the CH is reselected as per the proposed algorithm if the residual energy of the CH falls below the threshold.

The Cluster Head uses time-division multiplexing to receive information from its member. It collects the information and sends it to BS through image compression and transmission techniques over a secure channel. Even nearer CHs of different zones can communicate among themselves and one nearest to BS can send all related information. During the transmission, there can be depletion of energy which can be at the end of the member sensor node or CH. There can be chances that the energy of the current CH becomes below the threshold or any of its member nodes. In that case, the proposed scheme provides the following provision:

1. Reselection of Cluster Head
2. Selection of Super Cluster Head(SCH)

RESEARCH ARTICLE

Super cluster head is selected from among the various cluster heads using PROMTHEE as described in **Error! Reference source not found.**. All the cluster heads are required to periodically share the information regarding themselves and their complete zone to the SCH. The goal of super cluster head is to analyze the data shared and if any cluster head has the residual energy less than any of its nodes, then SCH sends a message to that particular CH and its members through selective flooding to reselect the CH.

3.3. Network Scenario

The cluster heads are positioned at the upper level whereas member nodes are placed at the lower level. The data is sent to the respective CH by lower-level member nodes. Data aggregated by CH is passed to BS, more energy is spent on sending data to longer distances by CH node. Later, CH cannot perform due to the consumption of high energy. To balance the energy utilization, CH is changed periodically. The following Figure 1 can explain the communication process between single hop (intra-cluster) and multi-hop (inter-cluster) communication.

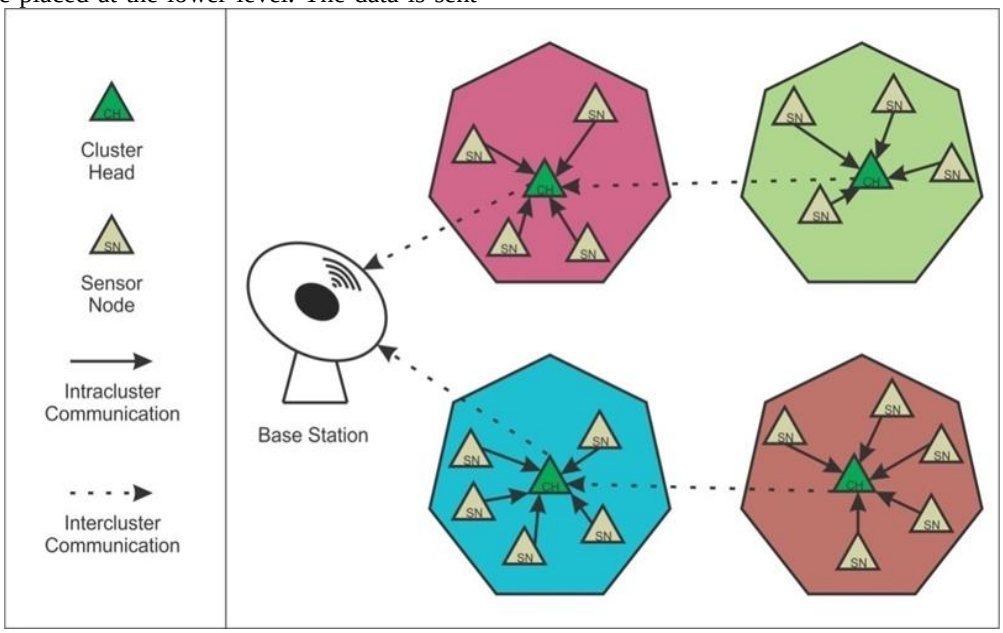

Figure 1 Network Scenario

1. Begin
2. Input pairwise comparison of IE, RE, ECR, AEN, DNCH
3. Calculate matrix sum of individual columns
4. Calculate the Eigen vector
5. Consistency Ratio(CR) is calculated from Consistency Index (CI) and Random index(RI) using the formula

   CR =CI/RI
6. Check the Consistency ratio.
7. If value of CR<0.1 then

   Pairwise matrix is reliable

   Else from repeat step 2

   End if

8. Calculate unweighted and weighted super matrix
9. End

Algorithm 1 CH Selection

1. Begin
2. Input weights of IE,RE,ECR,AEN,DNCH obtained from ANP
3. Input reference values of each criteria against the alternative.
4. Calculate:

   r(i,j)=[x(i,j)-min(x(i,j))]/[max(x(i,j)-min(i,j)] (for beneficial)

   r(i,j)=[max(x(i,j)-x(i,j)]/[max(x(i,j)-min(i,j)] (for non-beneficial)
5. Calculate the preference function

   Pj(a,b)=0 if R(a,j)<= R(b,j) i.e D(Ma-Mb)<=0

RESEARCH ARTICLE

Pj(a,b)=R(a,j)- R(b,j) if R(a,j)>= R(b,j) i.e D(Ma-Mb)>0

All negatives are replaced by 0

6. Calculate the aggregated preference function taking into account the criteria weights.

$$Pi(a,b)=[\sum wj.Pj(a,b)]/\sum wj$$

7. Determine the leaving and entering outranking flows
8. Calculate the net outranking flow for each alternative

End

Algorithm 2 Super CH Selection

3.4. Proposed Protocol

The protocol includes set of three phases, which are Registration, Login and Authentication. Table 2 describes the different notations used in the protocol.

Symbol	Description
SID	The unique identity of the sensor node
CID	Unique number for each node under a particular cluster
PID	Pseudo identity of the sensor node
RC	Unique request code
S	A base station encryption key
α, β	Unique random nonce
SK	Session key
H	Hash function
T, TS1,TS2,TS3,TS4	Time stamps

Table 2 Important Notations

3.4.1. Registration Phase

This phase deals with the node's registration under the base station. Primarily each and every sensor node carries a unique identification (SID) and a secret key. Every node sends its identity over a secure communication channel to BS. After that BS allocate a unique number $CID$to every node of the cluster. Two important keys- First a Master Key(for communication with CH), and a second Key that is shared with BS, are preloaded in every node. A hash function H which is one-way keyed is also loaded by BS.

When the deployment of sensor nodes finishes, BS forward the message to the SN containing pseudo-identity $H(PID)$ and unique request code RC i.e. $< PID, RC >$ where $PID = SID \oplus CID$. BS will get the SID of every node and encryption keys $= H(SID)$ to communicate.

As soon as the sensor node's deployment finishes, BS sends a list having details of sensor nodes of the clusters in the form of a message $< CID, RC, PID >$to all the CHs over a secure channel. BS takes the CID of every Cluster head and uses encryption key $x = H(CID)$for communication. With the same key, CH can also transmit information to the Base station. After every valid period, the Base station forwards restructured list to CH including transformed$< PID, RC >$, and member nodes are informed by CH in an encrypted form. BS always renewed the generator.

After following these means, every sensor node of the cluster gets a legitimate login. Assume node N1, N2 two sensor nodes of a specific cluster needs to converse with one another. Firstly, both will transmit a request to CH and play out the following steps for session key generation and mutual authentication.

3.4.2. Login Phase

During the login phase sensor node will forward a valid login appeal to the cluster head as described in Table 3. The following steps are performed:

Step1: The sensor node with identity SID computes $< H(PID), SID >$ and transmits the message.

Step 2: The Cluster head (CH) on receiving$< H(PID), SID >$, will check the validity of $H(PID), SID$ from the stored list. If the values are valid, it will encrypt the sensor id SID using MK=H(RC) and compute $E_{MK}H(SID)$ and sends $< E_{MK}H(SID), p, q, Q, G, E >$ back to the sensor node.

Step 3: On receiving $< E_{MK}H(SID), p, q, Q, G, E >$, the sensor node will compute $M1 = H(RC \oplus SID)$ and send $< M1 >$ back to the cluster head.

3.4.3. Authentication Phase

In this phase both the sensor nodes who wish to communicate with each other to exchange data such as text or images, will commonly validate each other and produce a secure fresh session key for encrypting their data and securing it from known attacks as presented in Table 4. The steps are:

Step-1: Sensor node $N1$ will generate a random nonce $\alpha \in Z_q^*$ and calculate the ECC point $A = \alpha.G$. After that, It will send the message $< A, TS1 >$ to the sensor node $N2$ where $TS1$ represents the present timestamp.

Step-2: On receiving$< A, TS1 >$ message, N2 will first verify the legality of the time stamp TS1 to avoid a replay attack. If found invalid, the process is terminated else continues. N2 will generate a random $\beta \in Z_q^*$ and compute the ECC point $B = \beta.G$ and the ECDLP point$C = \beta.A$. it will send its response to N2 $< B, TS2 >$, where $TS2$ is the current timestamp of N2.

RESEARCH ARTICLE

Step-3: On the reception of the response message $< B, TS2 >$ of N2, N1 will first check the validity of TS2. If invalid, the process is discontinued, otherwise, N1 will compute $D =$ Step-4: Once the response message $< M1, TS3 >$ is received, N2 will validate TS3, if invalid the process is terminated else continued. N2 will compute $M2 = SID_{N2} \| H(PID_{N2}) \| TS4$ and sends $< M2, TS4 >$message to N1.

$\alpha . B$ and $M1 = SID_{N1} \| H(PID_{N1}) \| TS3$. It then sends $< M1, TS3 >$message to N2.

Step 5: On getting the response message $< M2, TS4 >$, N1 and N2 will compute the session key independently using the parameters exchanged, i.e., $SK = h(D \| TS1 \| TS2)$ by N1 and $SK = h(C \| TS1 \| TS2)$ by N2.

Sensor Node (SN)	**Cluster Head (CH)**
computes *MK = H(RC)*	
	$< H(PID), SID >$ →
	checks the validity of H(PID),SID from the stored list if valid sends $E_{MK}H(SID),p,q,Q,G,E$
	← $< E_{MK}H(SID), p, q, Q, G, E >$
computes $M1 = H(RC \oplus SID)$	
	$< M1 >$ →

Table 3 Login Phase

Sensor Node (N1) SID_{N1}	**Sensor Node (N2)** SID_{N2}
generates random $\alpha \in Z_q^*$ computes $A = \alpha, G$	
	$< A, TS1 >$ →
	validates *TS1* generates random $\beta \in Z_q^*$ computes $B = \beta . G$ computes $C = \beta . A$
	← $< B, TS2 >$
validates *TS2* computes $D = \alpha . B$ computes $M1 = SID_{N1} \| H(PID_{N1}) \| TS3$	
	<*M1, TS3*> →
	validates TS3 computes $M2 = SID_{N2} \| H(PID_{N2}) \| TS4$
	← <*M2, TS4*>
$SK = h(D \| TS1 \| TS2)$	$SK = h(C \| TS1 \| TS2)$

Table 4 Authentication and Key Generation Phase

RESEARCH ARTICLE

Using the generated SK, the image is encrypted and transmitted to the other node.

3.4.4. Image Transmission using the Generated Session Key

Once the session key is generated mutually by the sensor nodes, data can be exchanged between both the nodes using the generated symmetric key $SK = h(C\|TS1\|TS2)$ as described in Figure 2 Image Transmission using the Generated Session Key Figure 2 . The nodes in communication can be a sensor node and CH or BS, and a cluster head.

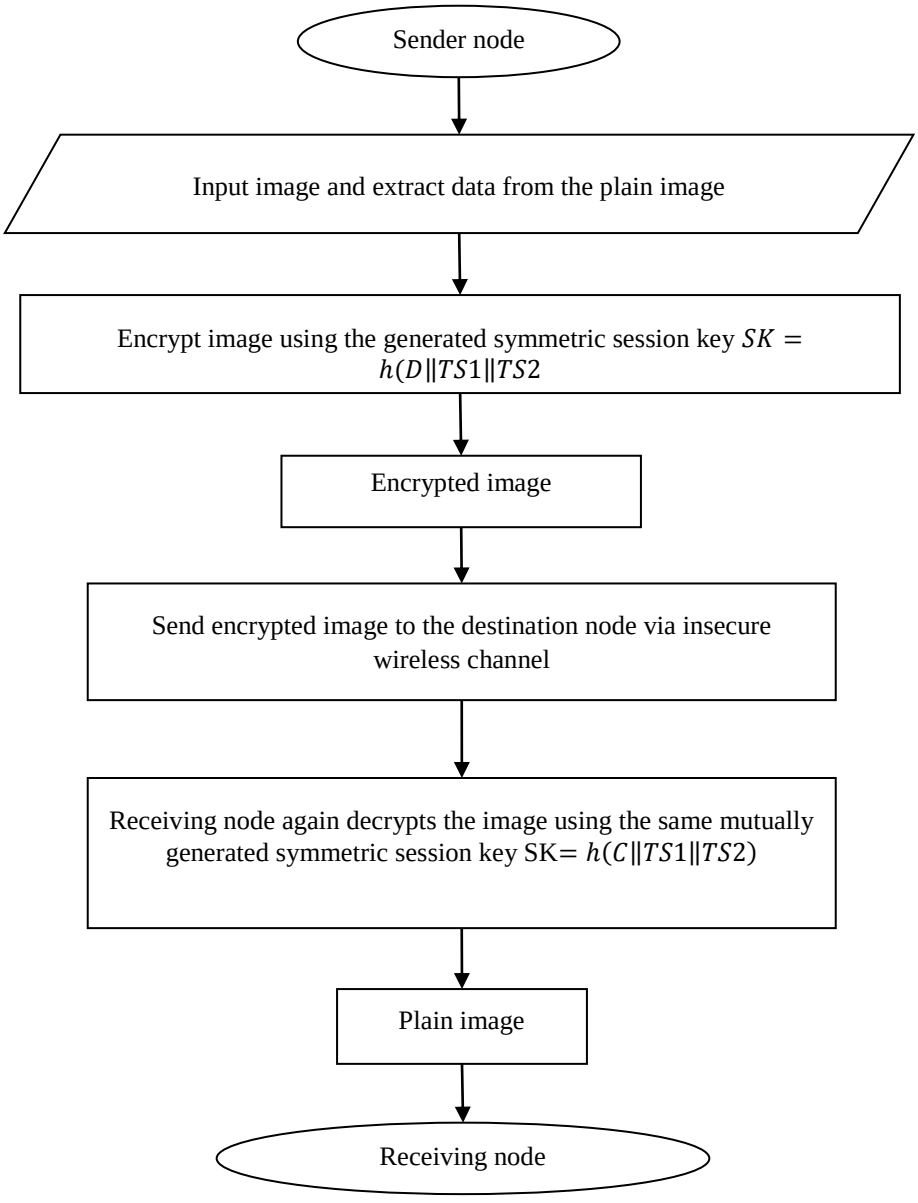

Figure 2 Image Transmission using the Generated Session Key

4. INFORMAL SECURITY ANALYSIS

The following section covers the informal protection testing of the anticipated protocol, which further depicts that the recommended protocol maintains the security of sensor data and has all the properties, which are obligatory for WSN communication.

RESEARCH ARTICLE

4.1. Provides Privacy Preservation

By using the mentioned protocol, the node's data is forwarded to a particular CH only that further collects the relevant data for transfer it to the base station. Consequently, no other node and CHs can access the data of an individual node. This allows the protection of the isolation of the individual sensor's data and eliminates data hacking probability.

4.2. Provides Confidentiality

During the data transmission, the messages/images are encrypted by using the generated session key $SK = h(C\|TS1\|TS2)$, which is symmetric. To communicate with the CH, BS, or sensor node, encryption of image or data is performed by sensor node by utilizing generated symmetric key $SK = h(C\|TS1\|TS2)$. Hence, all images/messages are transmitted to the destination nodes securely, thereby providing confidentiality.

4.3. Provides Mutual Authentication

In the above protocol, Key exchanged phase occurs without the involvement of any third party. Every one of the session keys is generated mutually within the communicating parties. At that point, the key is expressly validated by a common affirmation session key $SK = h(C\|TS1\|TS2)$. During data transfer phase, respective keys $SK = h(C\|TS1\|TS2)$are utilized for the encryption of image/data and destination validates the received data depending upon the timestamp, ID, and shared key.

4.4. Resists HELLO Flood Attack

During this attack, HELLO packets are transmitted by attackers to the sensor nodes with aim of consuming the resources of the sensor nodes. In this protocol, BS periodically sends a message comprising of a list of secret parameters of each node in the cluster to all the cluster heads in a secure manner. Hence, the proposed protocol resists the HELLO flood attack as the nodes will be able to defend it by first checking a valid cluster head sends the validity of the received message or not. Base station authenticates the node for data transmission.

4.5. Resists Compromised Cluster Head Attack

In this assault, the invader tries to compromise a cluster head to extract sensor nodes' data to derive sensitive node information/parameters. In the proposed protocol, CH forwards the encrypted form of data received from the member nodes to the BS. Therefore, the future protocol can defend against the compromised cluster head attack.

4.6. Resists Insertion Attack

Suppose an assailant tries to amend a few messages and interleave a tweaked message to the correspondence channel with the goal that an incorrect message is passed to the collector. The proposed protocol resists this attack since the invader needs to be acquainted with the shared session key $SK = h(C\|TS1\|TS2)$for a specific session. To know the shared session key, the attacker should have awareness about the secret parameter C, that is not shared on the communication channel. Because of the unavailability of the session key, the attacker cannot modify the message. Replacement of the message is possible, but it is impossible to create the same signed message.

5. PERFORMANCE ANALYSIS

This segment covers the performance study of the future authentication method for key agreement in terms of attack resistance, safety features, and some real-time metrics used in WSN.

To compute the computational costs, the notation T_h represents computation time of hash', T_{PA} represents addition computation time for the elliptic curve point ', T_{PM} represents 'the multiplication computation time of elliptic curve point ', and T_e denotes 'time for symmetric encryption/decryption'. Computational Cost comparisons for the three phases are shown in Table 5.

Computational Load	Chaterjee et al. [10]	Das[36]	Kumar et.al[35]	Proposed protocol
Registration phase	$1T_h + 2T_e$	$2T_h$	$3T_h$	$2T_h + 1T_e$
Login phase	$1T_h + 1T_E + 1T_{PA} + 1T_{PM} + 2T_e$	$3T_h$	$3T_h$	$1T_h + 1T_{PA} + 1T_{PM} + 2T_e$
Authentication & key generation phase on each side	$2T_h + 2T_{PM} + 2T_{PA} + 1T_E + 3T_e$	$5T_h$	$7T_h$	$2T_h + 2T_{PM} + 2T_{PA} + 2T_e$
Total computation time	$4T_h + 3T_{PM} + 3T_{PA} + 2T_E + 7T_e$	$10T_h$	$13T_h$	$5T_h + 3T_{PM} + 3T_{PA} + 5T_e$

Table 5 Computational Cost Comparison

RESEARCH ARTICLE

Attacks	Chatterjee et al.[10]	Benenson et al. [33]	Yeh et al. [34]	Kumar et al. [35]	Das [36]	Proposed protocol
Privacy preservation	'No'	'No'	'No'	'Yes'	'Yes'	'Yes'
Mutual authentication	'Yes'	'Yes'	'No'	'No'	'No'	'Yes'
'Confidentiality'	''Yes''	'Yes'	'Yes'	'Yes'	'Yes'	'Yes'
Hello Flood attack	'Yes'	'Yes'	'Yes'	''Yes'	'Yes'	'Yes'
Compromised CH attack	'No''	'No''	'No''	'Yes'	'Yes'	'Yes'
'Man-in-the-middle attack'	'Yes'	'No'	'Yes'	'Yes'	'No'	'Yes'
Insertion attack	'Yes'	'No'	'No'	'Yes'	'No'	'Yes'

Table 6 Security Features and Attack Resistance Comparison of the Proposed Scheme with Existing Protocols

Table 6 shows the evaluation of the recommended protocol in terms of resistance to several potential attacks. The comparison represents that the projected scheme is opposed to all the known attacks such as the hello flood attack, compromised cluster head attack. The protocol by Benenson et al.[33] Fails against Man-in-middle attack, insertion attack, and node compromise attack. Yeh et al.[34]protocol fails to provide security against compromised CH attack, insertion attack. Kumar et al.[35] Protocol successfully handle Hello flood, compromised cluster head, Man-in-middle, and insertion attack. Das[36]fail to provide security against insertion attacks and Man-in-middle attack.

Table 6 also depicts the comparison of the proposed protocol as far as security features provided. Our proposed scheme can provide all the necessary safety characteristics such as privacy preservation, confidentiality, mutual authentication, etc.

6. FORMAL SECURITY VERIFICATION USING AVISPA

Extensive use of the internet and wireless communication lead to the development of many new security protocols. To find the flaws of security protocols and to enhance the security level, there is an extreme requirement of the tools that can help to analyze these protocols and can also establish their correctness. For the analysis of medium to small-scale protocols, many semi-automated tools exist in the literature. However, for large scale internet security protocols, AVISPA tool provide suitable support. It includes high-level protocol specification language (HLPSL) which has capability to be modular and expressive and role-based also. It helps to analyze various protocols varying from falsification of protocols to abstraction based verification methods. Users can specify a security problem to the tool in HLPSL. AVISPA automatically translates the 'problem into an Intermediate Format IF'. Most of the available back-ends easily understand this intermediate IF language and are used to test and analyze various properties of protocols. Figure 3 shows the four back-ends which have been integrated into the tool [40].

Output Format (OF) is produced from the above back-ends, which consists of the summary, detail of the settings of protocol, proposed protocol name, back end used and goal of the analysis. The framework of the AVISPA tool is shown in Figure 4.

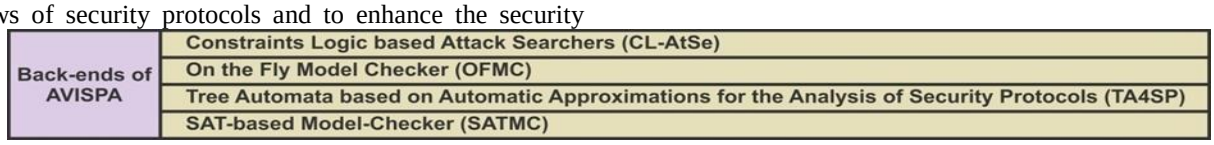

Figure 3 Back Ends of AVISPA

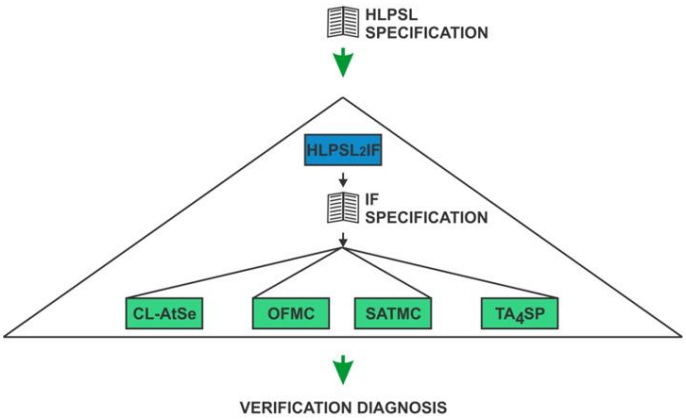

Figure 4 Structure of AVISPA[40]

RESEARCH ARTICLE

6.1. Results of Simulation

Most commonly used back-ends OFMC and CL-AtSe have been used for the simulation purpose. For the affirmation of replay assault, both the back ends performs a passive intruder search to ensure protocol execution by legal agents. Followed by this, back-ends notify the intruder with information of some normal sessions between the legal agents. For the 'Dolev–Yao model checking', OFMC and CL-AtSe also confirm the presence of any man-in-the-middle assault. Figure 5 and Figure 6 reveal the results of simulation of both the back-ends which clearly exhibit the safety of proposed protocol against man-in-the-middle and replay attacks.

```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/avispa/web-interface-computation
./tempdir/workfile77qXob.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATSTICS
parseTime: 0.00s
searchTime: 0.10s
visitedNodes: 18 nodes
depth: 4 plies
```

Figure 5 OFMC Simulation Analysis Results

```
SUMMERY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL
PROTOCOL
/home/avispa/web-interface-computation/
./tempdir/workfile77qXob.if
GOAL
As Specified
BACKEND
CL-AtSe
STATISTICS
Analysed: 8 states
Reachable: 8 states
Translation: 0.02 seconds
Computation: 0.01 seconds
```

Figure 6 CL-AtSe Simulation Analysis

7. CONCLUSION

With the acceleration in IOT and IOE, everything will be always best connected to the Internet allowing one to connect to anything at home, in the office, and so on. Sensors will be utilized with IoT to associate these things remotely for moving information. This means vast data in the form of text, images will be exchanged between devices leading to security risks. In this paper, a protected ECC based verification and key agreement scheme have been explained for secure image transmission in WSNs. The recommended scheme is protected, competent, and suitable for many IoT applications which are WSN-based. The informal security analysis of the proposed model proves that the protocol provides the desired safety qualities such as mutual authentication, confidentiality, fair key agreement, data integrity, perfect forward secrecy, etc. Also, the protocol is protected against hello flood attack, DoS attack, 'man-in-middle attack,' etc. Results received from Simulation tool AVISPA confirm the safety of the protocol against the known attacks. The performance comparison also proves the superiority of the proposed security model over the earlier schemes.

REFERENCES

[1] J. Ramasamy and J. S. Kumaresan, "Image Encryption and Cluster Based Framework for Secured Image Transmission in Wireless Sensor Networks," Wirel. Pers. Commun., vol. 112, no. 3, pp. 1355–1368, 2020, doi: 10.1007/s11277-020-07106-7.

[2] A. Durresi, V. Paruchuri, R. Kannan, and S. S. Iyengar, "Data Integrity Protocol for Sensor Networks," Int. J. Distrib. Sens. Networks, vol. 1, no. 2, pp. 205–214, 2005, doi: 10.1080/15501320590966459.

[3] W. Wang, D. Peng, H. Wang, H. Sharif, and H. H. Chen, "Energy-constrained quality optimization for secure image transmission in wireless sensor networks," Adv. Multimed., vol. 2007, pp. 1–9, 2007, doi: 10.1155/2007/25187.

[4] Sachin Gajjar, Mohanchur Sarkar and Kankar Dasgupta. Article: Cluster Head Selection Protocol using Fuzzy Logic for Wireless Sensor Networks. International Journal of Computer Applications 97(7):38-43, July 2014.

[5] D. Sharma, A. P. Bhondekar, A. Ojha, A. K. Shukla, and C. Ghanshyam, "A traffic aware cluster head selection mechanism for hierarchical wireless sensor networks routing," 2016 4th Int. Conf. Parallel, Distrib. Grid Comput. PDGC 2016, pp. 673–678, 2016, doi: 10.1109/PDGC.2016.7913207.

[6] A. B. Kaimal, S. Manimurugan, and C. S. C. Devadass, "Image Compression Techniques : A Survey," Int. J. Eng. Invent., vol. 2, no. 4, pp. 26–28, 2013.

[7] L. Sha, W. E. I. Wu, and B. Li, "Novel Image Set Compression Algorithm Using Rate-Distortion Optimized Multiple Reference Image Selection," IEEE Access, vol. 6, pp. 66903–66913, 2018, doi: 10.1109/ACCESS.2018.2879378.

[8] R. Naveen, "An Improved Image Compression Algorithm Using Wavelet and Fractional Cosine Transforms," Int. J. Image, Graph. Signal Process., vol. 10, no. 11, pp. 19–27, 2018, doi: 10.5815/ijigsp.2018.11.03.

[9] G. S. Rao, G. V. Kumari, and B. P. Rao, "Image Compression Using Neural Network for Biomedical Applications," Soft Comput. Probl. Solving. Springer, Singapore, pp. 107–119, 2019, doi: 10.1007/978-981-13-1595-4.

[10] K. Chatterjee, A. De, and D. Gupta, "A Secure and Efficient Authentication Protocol in Wireless Sensor Network," Wirel. Pers. Commun., vol. 81, no. 1, pp. 17–37, 2015, doi: 10.1007/s11277-014-2115-2.

[11] D. De Oliveira Gonçalves and D. G. Costa, "A survey of image security in wireless sensor networks," J. Imaging, vol. 1, no. 1, pp. 4–

RESEARCH ARTICLE

30, 2015, doi: 10.3390/jimaging1010004.
[12] M. Elhoseny, H. Elminir, A. Riad, and X. Yuan, "A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption," J. King Saud Univ. - Comput. Inf. Sci., vol. 28, no. 3, pp. 262–275, 2016, doi: 10.1016/j.jksuci.2015.11.001.
[13] A. Mehmood, M. M. Umar, and H. Song, "ICMDS: Secure inter-cluster multiple-key distribution scheme for wireless sensor networks," Ad Hoc Networks, vol. 55, pp. 97–106, 2017, doi: 10.1016/j.adhoc.2016.10.007.
[14] Y. H. B, Z. Aliouat, S. Harous, and A. Bentaleb, on Elliptic Curve Cryptography, vol. 1. Springer International Publishing.
[15] K. Gupta, S. Silakari, R. Gupta, and S. A. Khan, "An ethical way for image encryption using ECC," 2009 1st Int. Conf. Comput. Intell. Commun. Syst. Networks, CICSYN 2009, pp. 342–345, 2009, doi: 10.1109/CICSYN.2009.33.
[16] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," Proc. - IEEE Symp. Secur. Priv., vol. 2003-Janua, pp. 197–213, 2003, doi: 10.1109/SECPRI.2003.1199337.
[17] Zhang, Z., Wang, H., Vasilakos, A. V., & Fang, H. (2012). ECG-cryptography and authentication in body area networks. IEEE Transactions on Information Technology in Biomedicine, 16(6), 1070-1078.
[18] Isawa, R., & Morii, M. (2011). One-time password authentication scheme to solve stolen verifier problem. In Proceedings of the Forum on Information Technology (pp. 225-228).
[19] T. PonSelvalingam, S. Mahalakshmi, and S. Kurshid Jinna, "Re-authentication in Wireless Sensor Network," Int. J. Comput. Appl., vol. 55, no. 8, pp. 32–41, 2012, doi: 10.5120/8777-2720.
[20] Watro, Ronald, Derrick Kong, Sue-fen Cuti, Charles Gardiner, Charles Lynn, and Peter Kruus. "TinyPK: securing sensor networks with public key technology." In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 59-64. 2004. doi: 10.1145/1029102.1029113.
[21] E. Mykletun, J. Girao, and D. Westhoff, "Public key based cryptoschemes for data concealment in wireless sensor networks," IEEE Int. Conf. Commun., vol. 5, no. c, pp. 2288–2295, 2006, doi: 10.1109/ICC.2006.255111.
[22] L. B. Oliveira et al., "SecLEACH-On the security of clustered sensor networks," Signal Processing, vol. 87, no. 12, pp. 2882–2895, 2007, doi: 10.1016/j.sigpro.2007.05.016.
[23] D. Wu, G. Hu, G. Ni, W. Li, and Z. Zhang, "Research on secure routing protocols in wireless sensor networks," Chinese J. Sensors Actuators, vol. 21, no. 7, pp. 1195–1201, 2008.
[24] Raj, E. D. (2012). An Efficient Cluster Head Selection Algorithm for Wireless Sensor Networks–Edrleach. IOSR Journal of Computer Engineering (IOSRJCE), 2(2), 39-44.
[25] S. Sahraoui, Somia; Bouam, "Secure Routing Optimization in Hierarchical Cluster-Based Wireless Sensor Networks," Int. J. Commun. Networks Inf. Secur., vol. 5, no. 3, pp. 178–185, 2013.
[26] Biswas, K., Muthukkumarasamy, V., & Singh, K. (2014). An encryption scheme using chaotic map and genetic operations for wireless sensor networks. IEEE Sensors Journal, 15(5), 2801-2809.
[27] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," J. Netw. Comput. Appl., vol. 76, pp. 37–48, 2016, doi: 10.1016/j.jnca.2016.10.001.
[28] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless," Inf. Sci. (Ny)., vol. 321, pp. 263–277, 2015, doi: 10.1016/j.ins.2015.02.010.
[29] Elhoseny, M., Farouk, A., Batle, J., Shehab, A., & Hassanien, A. E. (2017). Secure image processing and transmission schema in cluster-based wireless sensor network. In Handbook of research on machine learning innovations and trends (pp. 1022-1040). IGI Global.
[30] Shankar, K., & Elhoseny, M. (2019). Secure Image Transmission in Wireless Sensor Network (WSN) Applications. Springer International Publishing.
[31] Sumalatha, M.S., Nandalal, V. An intelligent cross layer security based fuzzy trust calculation mechanism (CLS-FTCM) for securing wireless sensor network (WSN). J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-01834-1
[32] C. T. Chen, C. C. Lee, and I. C. Lin, "Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments," PLoS One, vol. 15, no. 4, pp. 1–28, 2020, doi: 10.1371/journal.pone.0232277.
[33] Benenson, Z., Gedicke, N., & Raivio, O. (2005). Realizing robust user authentication in sensor networks. Real-World Wireless Sensor Networks (REALWSN), 14, 52.
[34] H. L. Yeh, T. H. Chen, P. C. Liu, T. H. Kim, and H. W. Wei, "A secured authentication protocol for wireless sensor networks using Elliptic Curves Cryptography," Sensors, vol. 11, no. 5, pp. 4767–4779, 2011, doi: 10.3390/s110504767.
[35] Kumar, P., Sain, M., & Lee, H. J. (2011, February). An efficient two-factor user authentication framework for wireless sensor networks. In 13th International Conference on Advanced Communication Technology (ICACT2011) (pp. 574-578). IEEE.
[36] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Improved two-factor user authentication in wireless sensor networks," 2010 IEEE 6th Int. Conf. Wirel. Mob. Comput. Netw. Commun. WiMob'2010, vol. 8, no. 3, pp. 600–606, 2010, doi: 10.1109/WIMOB.2010.5645004.
[37] D. Mishra, A. Kumar, and S. Mukhopadhyay, "Expert Systems with Applications A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards," Expert Syst. Appl., vol. 41, no. 18, pp. 8129–8143, 2014, doi: 10.1016/j.eswa.2014.07.004.
[38] Khan, M. K., & Zhang, J. (2007). Improving the security of 'a flexible biometrics remote user authentication scheme'. Computer Standards & Interfaces, 29(1), 82-85.
[39] R. Dalia and R. Gupta, "Cluster Head Selection Technique for Improving The Network Lifetime in WSN using ANP," SSRN Electron. J., pp. 1–6, 2020, doi: 10.2139/ssrn.3564867.
[40] A. Armando, D. Basin, J. Cuellar, M. Rusinowitch, and L. Viganò, "AVISPA: Automated Validation of Internet Security Protocols and Applications," ERCIM News, vol. 64, 2006.

Authors

Rekha is working as an Assistant Professor of Computer Science and IT in Apeejay College of Fine Arts, Jalandhar, Punjab, India. She received her MCA degree from Guru Nanak Dev University, Amritsar, Punjab in 1998. Currently, she is working and pursuing her Ph.D. degree from Department of Computer Science and Engineering, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala. Her research interests include wireless sensor network and information security and image processing. She published several papers in journals and conferences.

Rajeev Gupta has 15+ years of teaching, research and software development experience. He is currently working in the Department of Computer Science and Engineering, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala. His areas of research specialization are Image processing, Internet of Things, WSN and Mobile Ad-hoc Network. He is an Associate Life Member of Computer Society of India (CSI), Member of International Association of Engineers (IAENG) and Middle East Association of Computer Science and Engineering (MEACSE).