Wireless Personal Communications (2023) 130:2935–2957
https://doi.org/10.1007/s11277-023-10410-7

Secure Key Management and Mutual Authentication Protocol for Wireless Sensor Network by Linking Edge Devices using Hybrid Approach

Sharmila[1] · Pramod Kumar[2] · Shashi Bhushan[3] · Manoj Kumar[4,6] · Mamoun Alazab[5]

Accepted: 22 March 2023 / Published online: 10 April 2023

Abstract
Wireless Sensor Networks (WSNs) play a crucial role in developing the Internet of Things (IoT) by collecting data from hostile environments like military and civil domains with limited resources. IoT devices need edge devices to perform real-time processing without compromising the security with the help of key management and authentication schemes. The above applications are prone to eavesdropper due to cryptographic algorithms' weaknesses for providing security in WSNs. The security protocols for WSNs are different from the traditional networks because of the limited resource of sensor nodes. Existing key management schemes require large key sizes to provide high-security levels, increasing the computational and communication cost for key establishment. This paper proposes a Hybrid Key Management Scheme for WSNs linking edge devices which use Elliptic Curve Cryptography (ECC) and a hash function to generate key pre-distribution keys. The Key establishment is carried out by merely broadcasting the node identity. The main reason for incorporating a hybrid approach in the key pre-distribution method is to achieve mutual authentication between the sensor nodes during the establishment phase. The proposed method reduces computational complexity with greater security and the proposed scheme can be competently applied into resource constraint sensor nodes.

Keywords Wireless Sensor Networks · Edge computing · Security · Computing · Cryptographic · Authentication

1 Introduction

Wireless Sensor Networks (WSNs) have been used in numerous fields like monitoring hostile environments, armed and civil domains in a short span of time. The sensor nodes are highly resource constrained in terms of energy, memory, transmission range, communication and computational capability. Compared to all these resources, energy is considered as an important factor to increase the lifetime of the network. The sensor nodes are deployed in hostile environment which are powered by battery and thus have limited energy.

✉ Manoj Kumar
wss.manojkumar@gmail.com

Extended author information available on the last page of the article

MICA2 mote [2–5] consists of microcontroller 8 bit AT Mega 128L, 250 Kbits/s data rate, 512Kbyte flash memory and 3.3 V on board battery with 2A-hr capacity. For MICA2 mote, size of battery is 3.3 V which should be used efficiently. A sensor node consists of both volatile and non-volatile memory with reduced memory size. The Sensor node information such as node Identity (ID), routing table information, security related data and program are stored in non-volatile memory. Due to the limited memory size, the program and application specific information must not be overloaded. The transceiver consumes more energy compared to all other operation of sensor nodes. While designing protocols for wireless sensor networks, the number of message transmission between the nodes should be minimized to attain the goal without negotiating the objectives of the WSNs.

With the rapid increase of IoT applications and their demands the cloud computing has been used to satisfy the needs of IoT. To addresses the challenges of using cloud computing for IoT, the edge computing has been introduced. The edge computing devices are installed near to the WSNs which usually one hops away. Edge computing for WSNs is a shows potential framework which supports low powered sensor networks to perform complex computational tasks. The general architecture of edge linked wireless sensor network architecture is shown in Fig. 1. As compared with traditional WSN system architectures, the proposed edge computing based architecture reduces the response time as well as bandwidth between the wireless sensor networks and cloud. The edge layer is physically close to WSNs.

The edge device has less capacity than cloud servers; still it handles a significant function of IoT demands. The edge node improves response time, privacy and reduces consumption of bandwidth [6–8, 42]. Some function of sensor nodes are to be outsourced to edge servers in the edge architecture, the secure communication must be ensured between sensor nodes and edge node. The cloud servers are more powerful which spend high resources for security [9, 10, 43]. In recent years, the edge computing has proved an effective assistance for WSNs. Therefore the security solutions proposed for cloud servers are not suitable for edge and sensor networks.

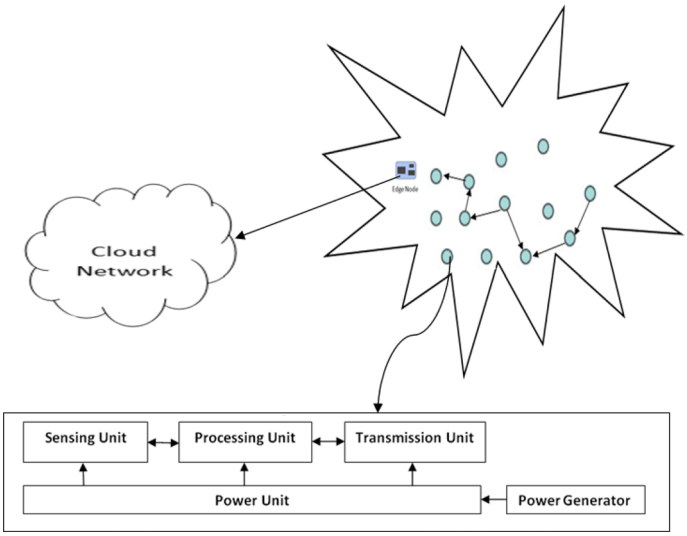

Fig. 1 General architecture of WSNs linked edge computing

The sensor nodes placed in an unfriendly location are prone to the node compromise attack [1–5]. As the sensor node communicates wirelessly, it is easy for an attacker to compromise the nodes' communication. To overcome the attacks of the WSNs, security must be integrated with the network. Providing security in WSNs is thought-provoking due to sensor nodes' resource constraint nature, but secure communication can play a significant role in avoiding different attacks. The security in WSN can be achieved with encryption and authenticating the communication among the sensor nodes. The limitations mentioned above can be avoided with the aid of a key management scheme. Secure communication is very important to endure the different types of malicious attacks. Security is achieved by means of encryption and authentication communication between the sensor nodes. Due to the resource constraint nature of sensor nodes, the traditional cryptographic methods are not appropriate for wireless sensor nodes. These problems are overcome by means of basic essential scheme called key management scheme.

A key management scheme can be widely utilized to secure communication between the sensor nodes within its range. The key management scheme is divided into 3 phases-key pre-distribution, shared key discovery, and key establishment [6–10]. Initially, the keys are pre-distributed into the sensor nodes (i.e., before node deployment).Once nodes are placed in the field, each node tries to determine a shared key within its communication range. During the second phase, the neighboring sensor nodes form a shared key for secure communications.

In recent times, numerous key management schemes have been suggested to establish secure communication among the sensor nodes during the network formation. Each of these schemes has its advantages and limitations. The suitable key management scheme should satisfy three important metrics [11–13]: security, efficiency, and flexibility. The main motivation of the proposed work is as follows: The rising need of new in-formation processing paradigm such as health monitoring, environment monitoring and surveillance tasks have led to massive active research in the fields of highly distributed sensor networks. This dissertation is especially useful in catastrophic or emergency situation where human intervention may be dangerous. The failures of WSNs are inevitable due to hostile environment and unattended deployment; therefore sensor nodes must operate potentially in large numbers and with greater security. The national border security and disaster management theme is the need for this research in secure key management and routing of secure data in wireless sensor networks. The sensor nodes are highly resource constrained; providing security for WSNs is still a challenging task. Secure end to end relationship does not scale well in large scale WSNs [14–25].

Traditional cryptographic techniques are not suitable for resource constrained WSNs. A viable alternative is to use key management scheme. Many key management schemes are developed to fulfill their requirements for key establishment in wireless sensor networks. Still, it faces many problems such as increased memory requirement, computational and communication cost.

The limitations of the existing key pre-distribution schemes depend on symmetric and asymmetric cryptographic techniques are as follows:

- The major limitation of Elliptic Curve Cryptography (ECC) [18, 32] based key pre-distribution schemes is that the keys are generated directly using ECC and pre-distributed into the sensor node. This increases communication costs and the requirement of memory. The key establishment between the sensor nodes is not addressed in the existing ECC-based key pre-distribution scheme.

- The Random Seed Distribution with Transitory Master Key scheme (RSDTM) [21, 22] is the Random Seed Distribution's major limitation because a node cannot establish a shared key after a certain time. If an adversary captures anode's master key, then the entire network can be compromised by an attacker.
- In E–G scheme [19], the sensor nodes need to store a vast number of keys to increase sensor networks' connectivity. However, it provides neither authentication nor key revoking between sensor nodes. Moreover, the scheme requires more memory for key storage.

This paper's main contribution is to overcome the above limitations; the proposed key management Scheme for WSNs linked edge node to reduce memory requirement, computational and communication overhead. The edge node is used to generate a unique key seed key from elliptic curve and shared with sensor nodes. It integrates both the cryptography techniques to achieve a high level of security and improves a node-to-node authentication compared to the existing key management scheme such as E–G and RSDTM.

The structure of the paper is arranged as follows: Sect. 2 reviews the related works of existing security schemes for WSNs. Section 3 explains the proposed scheme by integrating the authentication and secure key establishment using a hybrid approach. Section 4 describes the theoretical investigation of the proposed scheme. Section 5 reviews the simulation result and analysis of the proposed method. Section 6 summarizes the proposed method.

2 Related Works

The advantage of combining IoT with Edge servers are discussed in [44]. The processing of large volume of real-time data poses significant challenges in large scale IoT system. The above challenges are addressed with the help of edge computing [45] in resource constrained IoT nodes. Zhiwei Zhao et al. [46], addressed the challenges of deploying edge node in large scale IoT.

Generally key management plays vital role to provide security in any network [46–48]. In edge computing infrastructure, the key management scheme allows the nodes to establish a pairwise key to perform secure communication. The key management scheme for edge computing is attracting the attention of many researchers in recent years.

Eschenaueret al. [19] proposed the key management scheme based on the probabilistic method for WSNs. E–G scheme is depending on a random graph structure. This scheme is specially offered for wireless sensor networks. Most of the research work for WSNs is a framework of E–G methods. The major limitation of E–G scheme is no authentication, poor connectivity and periodic key refreshing is not done. The key should be refreshed periodically in order to overcome node compromised attacks. It does not support clustering operations to minimize the consumption of energy. The Q-composite method is the extension of EG-Scheme. The sensor nodes' network resilience is improved by using more keys instead of a single key in the EG scheme. The main advantage of this scheme is improved the resilience of network against node compromise attack. However, this scheme is more susceptible to attack once more numbers of nodes are compromised.

The pair wise key is generated by Blom's scheme [20]. The pairwise key is established among neighboring nodes in the network. It uses the threshold property to attain high resilience. The attacker needs to capture more nodes (i.e., greater than the threshold value) to

capture the whole network. When the threshold value increases, the storage space required to hoard the keys also increases. To secure the WSNs, several key management schemes have been suggested [21–30].

The symmetric pre-distribution scheme offers security efficiently but not appropriate for the unfriendly environment. Gandino et al. [21, 22] proposed a Random Seed Distribution with Transitory Master Key scheme (RSDTMK),in which the seed keys are stored inside the sensor nodes instead of plain keys. In the initialization phase, the node generates the pairwise key using the master key within the activated time period. The main limitation of this scheme is the key cannot be generated after the time-out period. If the attacker compromised the master key, eavesdrop on the entire key information within the initialization phase and discovers the entire pairwise key shared between the nodes.

Public key cryptography plays an important role in cryptographic techniques [31–34]. It has a private and public key. The key size of public-key cryptography needs to be high to offer a high level of security. The direct implementation of public-key techniques is not suitable for resource constraint sensor nodes.

Many research works have been carried out on resource constraint network using public-key cryptography. Asymmetric key cryptography techniques need to perform more computation for encryption and decryption operation. It needs more computational power and processing time for performing the operation. Rivest Shamir Adleman (RSA) algorithm uses 512 to 2048 bits as key size. Many research works [35–39] have been carried on Elliptic Curve Cryptography using 8-bit CPUs. As compared to RSA, the key size of ECC is small. TinyOS key pre-distribution method is depends on ECC. For the RSA algorithm, the key size is 1024 bits, whereas for ECC, the key size is 160 bits for secure communication.

The elliptic curve cryptography based key pre-distribution scheme [40, 41] is proposed for WSNs. The keys are generated by performing a point doubling operation. It offers high connectivity as well as resilience for the resource constraint nature of sensor nodes. This scheme's limitation is the plain keys (ECC points)are pre-distributed into the sensor node. The author did not address the issue of how the sensor nodes have established the key among the sensor nodes, and communication overhead is high. Du et al. [32] demonstrated routing-driven key management scheme using elliptic curve cryptography for WSN. This scheme's performance is carried out in heterogeneous sensor networks to achieve high-level security in WSNs. It establishes shared keys with neighbor nodes using ECC based digital signature.

One of the evolving techniques of cryptography is Hyper Elliptic Curve Cryptography(HECC). The security level of HECC is the same as RSA and ECC and the key size is 80 bits [31, 33, 34], whereas 1024 bit for RSA and 60 bits for ECC. Some recent studies can also be referred from [42–52].

The approaches above for WSNs emphasize the distribution of key between the sensor nodes and not on node-to-node authentication. Thus, in this paper, the hybrid key management scheme method is proposed by linking edge devices along with sensor nodes to provide authentication between nodes and reduce storage space, computational and communication overhead. The following are the limitations imposed by the existing key pre-distribution scheme based on symmetric and asymmetric cryptographic techniques:

- The major limitation of ECC based key pre-distribution scheme [30] is the keys that are generated directly and pre-distributed into the sensor node. The key establishment between the sensors nodes are not addressed in existing ECC based key pre-distribution scheme. Due to direct implementation of ECC, it increases memory requirement and communication overhead during the key establishment between the sensor nodes.

- The major limitation of Random Seed Distribution with Transitory Master Key scheme (RSDTM) [21, 22] is after the time out period a node cannot generate the shared key. If the adversary captured a master key of sensor node using the captured information entire network can be easily compromised by an attacker.
- E–G scheme [19] needs more memory to achieve high connectivity and resilience. There is no authentication process and key revoking between the sensor nodes. The pre-distribution of secret key over the large scale network is not feasible due to more number of keys need to be stored in sensor nodes to achieve high connectivity.

To overcome the above limitations, Hybrid Key Management Scheme is proposed for WSNs by linking edge computing node which will reduce memory requirement, computational and communication overhead. Hybrid Key Management scheme is an integration of symmetric and asymmetric based cryptography techniques which provides a node-to-node authentication and higher level of security when compared to existing key management scheme such as E–G and RSDTM.

3 Proposed Key Management Algorithm for WSNs

In the proposed hybrid key management scheme, key pre-distribution depends on ECC and a hash function. Before deploying sensor nodes, three offline and one online phase are performed, namely parameter selection for the elliptic curve, generation of unique seed key, identity-based key ring generation, key establishment, and mutual authentication phase. The edge device generate a unique seed key from the elliptic curve equation, which is preloaded to each sensor node, and a hash function is used on the seed key to generate the private key. Then, the generated key-ring and their corresponding identities are loaded into the sensor nodes memory. Once nodes are placed in the field, sensor nodes disseminate their ID to form common keys with other nodes. The nodes are mutually authenticated using their own identity of nodes without a huge communication overhead.

3.1 Parameter Selection for Elliptic Curve

Before sensor nodes deployment, the edge node generates the key pool using the Elliptic Curve Cryptography equation over an integer finite field. The elliptic curve parameters selection is vital in wireless sensor networks to reduce the number of links compromised by an attacker and improve network connectivity. The elliptic curve parameters p, a, and b are chosen where the value of prime number p should be greater than the total nodes deployed in the field. For example, if the number of nodes deployed in an area is 50, the prime number's value should be greater than 50 to improve the connectivity at the same time to increase the resilience.

3.2 Generation of Unique Keys

Unique keys are generated by edge node before sensor nodes are deployed in the area. Once the ECC equation's coefficients are chosen, the unique seed keys are produced for sensor nodes.

3.2.1 Key Pool Generation using ECC

Let the prime number $p = 59$ and let the constants $a = 1$ and $b = 1$. The first step is to verify the quadratic residue that:

$$4a^3 + 27b^2 modp \neq 04a^3 + 27b^2 modp = 4 \times 1^3 + 27 \times 1^2 modp$$

$$4a^3 + 27b^2 modp = 4 + 27mod43 = 31mod43$$

$$4a^3 + 27b^2 modp = 12 \neq 0$$

Then find the quadratic residues $\boldsymbol{Q}_{59}$ from the reduced set of residues $Z_{59} = \{1, 2, 3, \ldots \ldots, 57, 58\}$ as shown in Table 1.

Therefore, the group of $\frac{p-1}{2} = 28$, the quadratic residues are

$$Q_{59} = \{1, 3, 4, 5, 7, 9, 12, 15, 16, 17, 19, 20, 21, 22, 25, 26, 27, 28, 29, 35, 36, 41, 45, 46, 48, 49, 51, 53, 57\}$$

Table 1 Quadratic residues of Q_{59}

$x^2 modp$	$(p-x)^2 modp$	=
1^2 mod 59	58^2 mod 59	1
2^2mod 59	57^2 mod 59	14
3^2 mod 59	56^2 mod 59	9
4^2 mod 59	55^2 mod 59	16
5^2 mod 59	54^2 mod 59	25
6^2 mod 59	53^2 mod 59	36
7^2 mod 59	52^2 mod 59	49
8^2 mod 59	51^2 mod 59	5
9^2 mod 59	50^2 mod 59	22
10^2 mod 59	49^2 mod 59	41
11^2 mod 59	48^2 mod 59	3
12^2 mod 59	47^2 mod 59	26
13^2 mod 59	46^2 mod 59	51
14^2 mod 59	45^2 mod 59	19
15^2 mod 59	44^2 mod 59	48
16^2 mod 59	43^2 mod 59	20
17^2 mod 59	42^2 mod 59	53
18^2 mod 59	41^2 mod 59	29
19^2 mod 59	40^2 mod 59	7
20^2 mod 59	39^2 mod 59	46
21^2 mod 59	38^2 mod 59	28
22^2 mod 59	37^2 mod 59	12
23^2 mod 59	36^2 mod 59	57
24^2 mod 59	35^2 mod 59	45
25^2 mod 59	34^2 mod 59	35
26^2 mod 59	33^2 mod 59	27
27^2 mod 59	32^2 mod 59	21
28^2 mod 59	31^2 mod 59	17
29^2 mod 59	30^2 mod 59	15

Table 2 Quadratic residues of $y^2 \in Q_{59}$

x	0	1	2	3	4	5	6	7
y^2	1	3	11	31	10	13	46	56
$y^2 \in Q_{59}$	Y	Y	N	N	N	N	Y	N
y_1	1	11					20	
y_2	58	48					39	

Table 3 Seed keys for $E_{59}(1, 1)$

(0, 1)	(0, 58)	(1, 11)	(1.48)
(6, 20)	(6, 39)	(8, 7)	(8, 52)
(11, 24)	(11, 35)	(13, 21)	(13, 38)
(14, 24)	(14, 35)	(15, 21)	(15, 38)
(19, 25)	(19, 34)	(21, 16)	(21, 43)
(22, 13)	(22, 46)	(25, 4)	(25, 55)
(26, 27)	(26, 32)	(27, 8)	(27, 51)
(30, 56)	(30, 3)	(31, 21)	(31, 38)
(34, 35)	(34, 24)	(38, 10)	(38, 49)
(39, 8)	(39, 51)	(40, 12)	(40, 47)
(41, 13)	(41, 46)	(42, 26)	(42, 33)
(43, 14)	(43, 45)	(45, 4)	(45, 55)
(48, 4)	(48, 55)	(49, 17)	(49, 42)
(51, 22)	(51, 37)	(52, 8)	(52, 51)
(53, 29)	(53, 30)	(54, 15)	(54, 44)
(55, 13)		(55, 46)	

$y^2 = x^3 + x + 1 \ mod \ \ 59$ is computed and find out, if y^2 is in the group of quadratic residues Q_{59} as shown in Table 2.The elliptic curve points $E_p(a, b) = E_{59}(1, 1)$ are shown in Table 3.

For the prime number p = 59, approximately 62 points are generated. Each unique elliptic curve point is stored in sensor node before deployment. Once unique elliptic curve point is assigned to sensor nodes, the private key-ring is generated using point doubling and addition operation.

3.3 Identity Based Key Ring Generation

In this proposed scheme, the key-ring selection depends on the node's ID, unique seed key, and hash function. The identity-based key-ring selection has more advantages compared to the pseudo-random sequence [20, 22]. During the key establishment phase, the node has to interchange its identity for peer nodes to obtain the shared key. This also provides legitimacy of the entity. In the pre-deployment phase, the edge computing device assigns a unique identifier ID_i, hash functionh_j, and seed key $[u, v]$ to each sensor node.

The edge node randomly chooses ' m' other sensor nodes to generate the unique key-ring using a simple hash function and store the keys and their corresponding identities into the sensor node memory. The following Eq. 1 generates the key Ki.

$$K_i = h_j(u_i, v_i) \tag{1}$$

Consider an example as presented in Fig. 2, the sensor mote S_1 randomly selects three sensor nodes S_2, S_6 and S_8 from the network and generates the key-ring K_2, K_6 and K_8 using a hash function on their corresponding seed key and load the key indices and ID of the sensor nodes in key-pool. Similarly, it stores 'M' pairs of key and ID in the key-ring, where m is the key-ring size.

3.4 Key Establishment and Mutual Authentication Phase

Once the keys are distributed, the sensor nodes are randomly disseminated in the field. In the initialization step, each sensor node shares its ID_i and receives neighborhood nodes' ID.

Consider the nodes ID_j, which is in the range of sensor mote ID_i, verifying that the received ID_i belongs to the key-ringstored in the sensor node before the deployment. If it is in their key-ring, it chooses a timestamp to avoid replay attack and shares the joint request message to the corresponding node ID_i. Once the sensor node ID_i receives the joint request message, it computes C' and verifies that $C = C'$. If $C = C'$, the node is mutually authenticated and generated the session key by computing $S_k = K_i + K_j$. There are two cases in the key establishment phase, namely the direct and indirect key establishment phase. The algorithm is explained as follows,

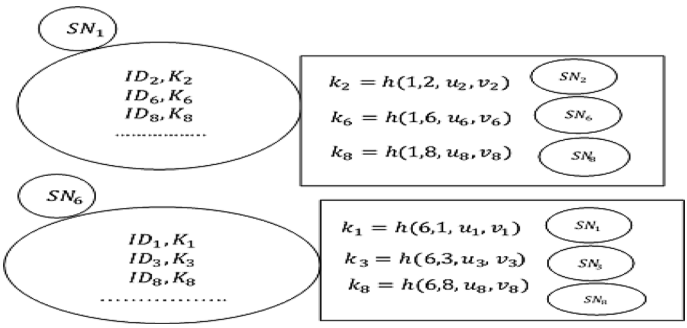

Fig. 2 Key predistribution of hybrid key management scheme

$Algorithm$:

$Input: ID\ of\ receiver\ sensor\ node\ ID_i$

$Output$: $Session\ key\ K_{ij}$

$Step: 1 \quad i \rightarrow *: < ID_i, T_1 >$

$Step: 2\ j = discover(ID_i \in m)$

$if\ (ID_i \in m)$

$C = h(K_1, ID_1)$

$j \rightarrow i: < ID_j, T_6, C >$

$Step: 3\ if\ (ID_i \in m)$

$C_1' = h(K_1, ID_1)$

$S_k = K_i \oplus K_j$

3.5 Case: 1 Direct key Establishment Between the Nodes

After sensor nodes are disseminated in the area, it broadcasts the unique ID and timestamp to the neighboring nodes within the broadcasting range. The sensor node which receives the neighbor information validates the timestamp to avoid the replay attack and checks the received identity as to whether it belongs to the key-ring or not. If the sensor node's identities belong to the key-ring, then it transmits $C = h(k_1, ID_1)$ where $k_1 = h(1, 6, u_1, v_1)$ and timestamp to node 1.

Node 1 receives the authentication message from node 6; it checks the timestamp and verifies its key-ring. If ID_6 belongs to the key-ring, SN_1 calculates the $C' = h(k_1, ID_1)$ and verifies if $C = C'$, then it authenticates node 6 and computes the session key $S_k = K_1 \oplus K_6$. Fig.3 shows the direct establishment of keys among the sensor nodes.

3.6 Case: 2 Indirect Key Establishments Between the Nodes

If the identity of the SN_1 does not belong to the key-ring, then the sensor node 6 computes D where $D = h(K_6, ID_1)$ and shares it to the sensor node 1. The sensor node 1 verifies the identity of sensor node 6, and if it belongs to the key-ring, it verifies $D' = D$ and authenticates node 6. Node 1 computes $'m'$, where $m = E_{K_6}(K_1)$ and transmits the value of $'m'$ and its identity to node 6. Node 6 decrypts the message with the help of K_6 and obtains the K_1. Then the session key is formed by $S_k = K_1 \oplus K_6$. Figure 4 shows the operation of indirect key establishment between the sensor nodes.

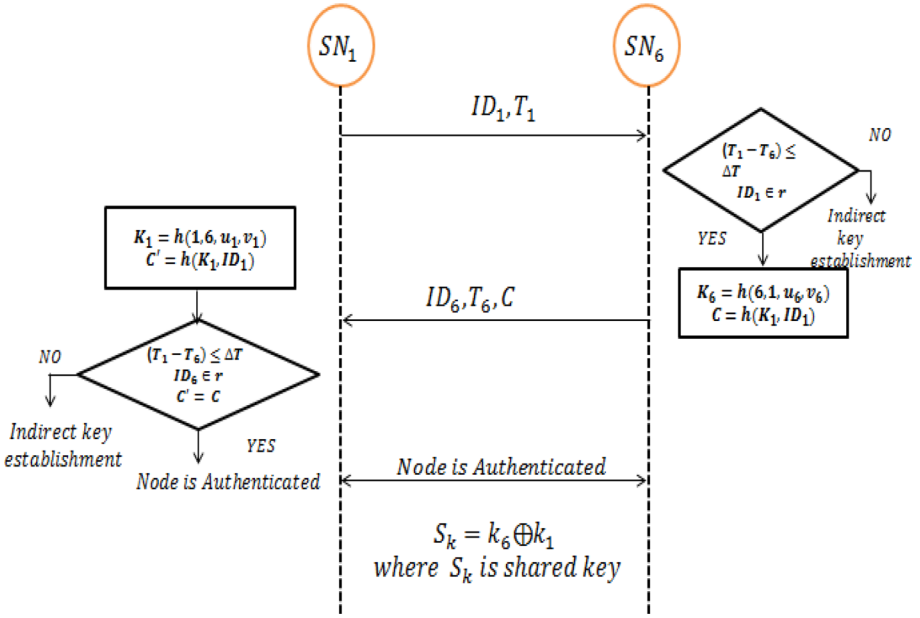

Fig. 3 Direct key establishment between the nodes

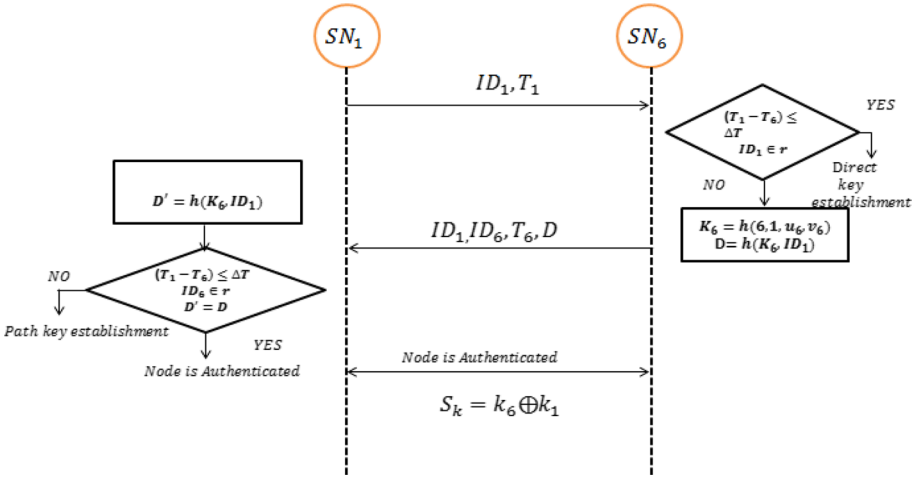

Fig. 4 Indirect key establishment between the nodes

3.7 Path Key Establishment

If the common key is not shared among the two nodes, it tries to establish a path key through an intermediate node using the same handshake protocol.

Table 4 Memory storage space required for shared key

Scheme	E–G[9]	RSDTMK[11]	ECC[21]	HKMS
Initial Storage	$r{\cdot}(l_k + l_{kID})$	$r{\cdot}l_s + l_k + r \cdot l_{sID} + l_s + l_p$	$r\left(K_i + l_{ID}\right)$	$r\left(K_i + l_{ID}\right)$
Working Phase	$r{\cdot}(l_k + l_{kID}) + v$ $(l_{ID} + l_{kID})$	$r{\cdot}\,(l_k \cdot l_{kID}) + v$ $(l_{ID} + l_{kID})$	$r{\cdot}(K_i + l_{IDk}) + v$ $(l_{ID} + l_{kID})$	$r\left(K_i + l_{ID}\right) + v(\left(K_{i,j}\right)$

Table 5 Communication efficiency

Scheme	Hops	Number of Messages	Size of transmitted data
E – G[9]	1	2	$(r+1) \cdot l_{KID} + 2 \cdot l_{ID} + l_k$
RSDTMK[11]	1	2	$r \cdot l_{SID} + l_{KID} + 2 \cdot l_{ID} + l_k$
HKMS	1	2	$3 \cdot l_{ID} + v \cdot l_{KID} + T_s$

4 Performance Analysis of the Proposed Hybrid Approach

The proposed system's effectiveness has been analyzed theoretically with the help of storage requirements and communication costs. The proposed scheme's performance is analyzed with the help of the parameters such as the number of nodes in the network, keys in the key pool, and hop count.

4.1 Memory Storage Requirement Analysis

The storage requirement has been analyzed to evaluate the efficiency of the protocol. The metrics that describe the efficiency of storage are key ring size (r), length of the seed key (l_s), key identifier (l_{kID}), length of the key (l_{UK}), and the number of neighbors (v).

Table 4 shows the storage space required to store the key material in sensor nodes. The following metrics can assess the memory capacity required for the proposed scheme, namely the key-size as 160 bits long, node ID 2 bytes, key-ring size of 10, the memory required to store the key information for the HKMS is 202 bytes, whereas in E–G scheme it is 220 bytes [19] and for the RSDTMK 316 bytes [21, 22]. The proposed scheme's storage capacity is 18 bytes less compared to the E–G and 114 bytes compared to the RSDTMK scheme.

4.2 Communication Efficiency

In this proposed scheme, finding the key among two nodes requires one-hop communication between nodes as in E–G and RSDTMK; but the message's size is different for each scheme. In HKMS, once nodes are disseminated in the field, it initiates the communication by sending a hello message containing the node and timestamp's identifiers. The acknowledged message contains the node's identifier, neighbor node identifier, and Message Authentication Code (MAC) of the message (c).

Table 5. shows the comparison of communication efficiency of EG, RSDTMK and HKMS.Considering the $l_k(MAC) = 16byte$, $l_{ID} = 2byte, l_{SID} = 2byte$, $r = 10$ and in E–G $l_{kID} = 2byte$ and RSDTMK $l_{kID} = 3byte$, RSDTMK needs 43 bytes to establish a pairwise key, whereas in E–G scheme, 42 bytes and HKMS requires only 26 bytes to establish a secure key establishment. From this theoretical analysis, it is inferred that the proposed HKMS requires a smaller number of bytes to form a secure communication between the sensor nodes (Table 6).

5 Simulation Results and Discussion

To assess the performance of the HKMS protocol, the NS 2.35 simulator has been used. The analysis is emphasized on the formation of the keys in the network. The definition of simulated parameters is as follows:

- Reduced Memory Requirement: The key management scheme should be designed in such a way that the node should occupy less amount of memory to store the secret keying information and identity of the sensor nodes [20].
- Communication Efficiency: For key establishment or updating, the amount of information exchanged among the neighbor nodes should be reduced in order to minimize energy consumption [11].
- Computation: The number of computation should be reduced during key establishment [11].
- Energy Efficiency: The number of message exchanged between the sensor nodes during the key establishment phase is reduced to minimize the energy consumption [11].
- Key Connectivity: The probability of secure link formed between the two sensor nodes. The probability of establishing the shared keys between the sensor nodes should be maximized [9].
- Resilience: Resilience is the resistance of sensor nodes against node capture attack. If an attacker compromises the legitimate node, the secret key information stored in the node should be confident [9].

Generally, the key establishment schemes are focused only on the generation and establishment of keys which does not provide mutual authentication and key exchange among the sensor nodes. The proposed key management's performance is analyzed in

Table 6 Simulation parameters and its value

Parameters	Values
Sensing area	1000 m X 1000 m
Number of nodes	100
Simulation time	20 secs
Initial energy	50 Joules
Radio propagation Model	Two Ray Ground model
MAC	IEEE 802.11
Antenna type	Omni antenna
Broadcast Interval	10 ms

terms of resilience, connectivity/channel existence of the network, network availability, broadcast delay, and energy consumption. The simulation parameters used to assess HKMS, E–G and RSDTMK are given in Table 3.

5.1 Connectivity Analysis for HKMS with E–G and RSDTMK

The connectivity is the establishment of a communication channel among two sensor nodes when they share a minimum of one key. The probability of secure link establishment among the two nodes [18] can be defined by Eq. 2,

$$P(i,j) = \left(\left(K_s - m\right)/m\right)/\left(K_s/m\right)\right) \tag{2}$$

The probability of link established between the sensor nodes in the network depends on the value of K_s and m; where K_s is key size and m is key-ring size. The value of m is the same for all the sensor nodes. Figure 5 shows that the probability of the link exists between the nodes disseminated in the network. From the resulting output, it is inferred that 100% of connectivity is achieved by the proposed scheme for the key-ring size of 10 whereas in E–G and RSDTMK were 10% and 80%, respectively for key-ring size of 10. The simulated results indicate that the proposed HKMS scheme increases 80% and 10% of connectivity compared with E–G and RSDTMK.

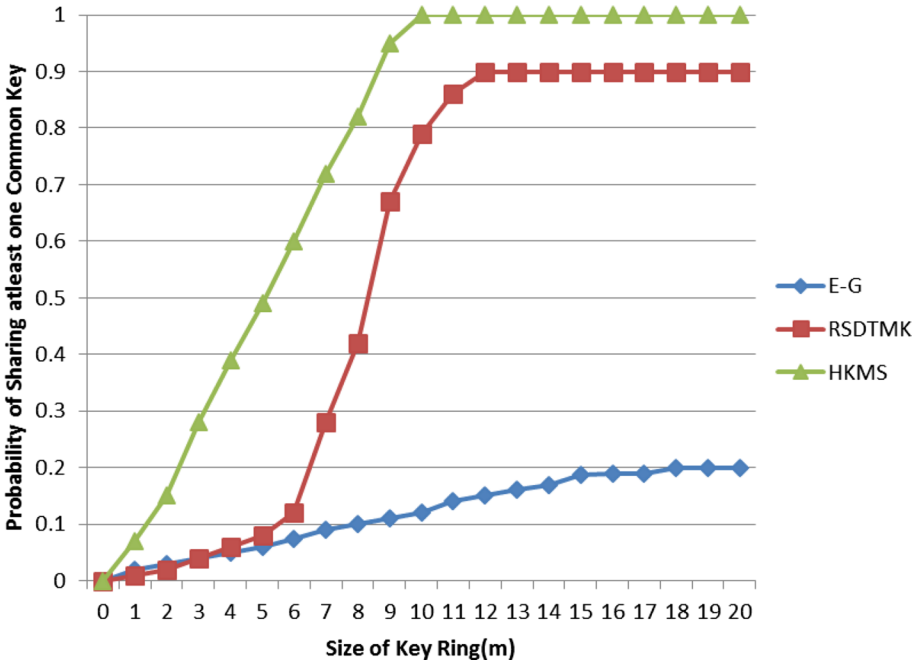

Fig. 5 Connectivity analysis of HKMS with E–G and RSDTMK

5.2 Comparison of Resilience for HKMS with E–G and RSDTMK

The resilience is defined as the ability to reduce the compromising of secret key materials loaded in the sensor nodes. Assuming that the link between sensor i and j is under the attack, the attacker compromises the link form a union $A = \{a_1, \ldots a_n\}$ of $a > 0$ means compromised sensor nodes.

The probability of key sharing among the node i and j is not present in the set A [22] is given by Eq. 3,

$$\overline{\Pr}(S_{i,j}) = \Pr\left[\left(m_i^1 \in m_j \wedge m_i^1 \notin A\right) \vee \ldots\ldots\ldots \left(m_i^k \in m_j \wedge m_i^k \notin A\right)\right] \tag{3}$$

The probability of the coalition of k trials can be given by Eq. 4,

$$\Pr\left(S_{i,j}\right) = 1 - \sum_{s=1}^{k} (-1)^{s+1} \binom{k}{s} \left(\binom{p-s}{k-s} / \binom{p}{m}\right) \left(\binom{p-s}{k-s} / \binom{p}{m}\right)^{a} \tag{4}$$

Figure 6 shows the probability of compromising a linkage between the sensor nodes by an attacker for different values of p, a and m and the network secured by the proposed method compared to the basic E–G and RSDTMK schemes. The simulation results show that the proposed scheme decreases the probability of links compromised between sensor nodes by 39% compared to the existing schemes.

In the E–G scheme, the attacker compromised 50% of a communication link in the network by capturing 10 sensor nodes that are minimal resistant to node capture attack. When the invader/attacker captures 50 to 60 nodes, the whole network is thoroughly compromised. In the proposed approach, the invader requires capturing more sensor nodes to compromise the link between the nodes. It provides more resistance against node capture attack even though the attacker knows the key-ring compromised node's key-ring. The key pool reconstruction is not possible because the key-rings are generated by one way hash function. In the initialization phase, the sensor node broadcasts its identity instead of sharing the seed key stored in the key-ring. The proposed HKMS abides against the node capture attack and provides mutual authentication between the sensor nodes.

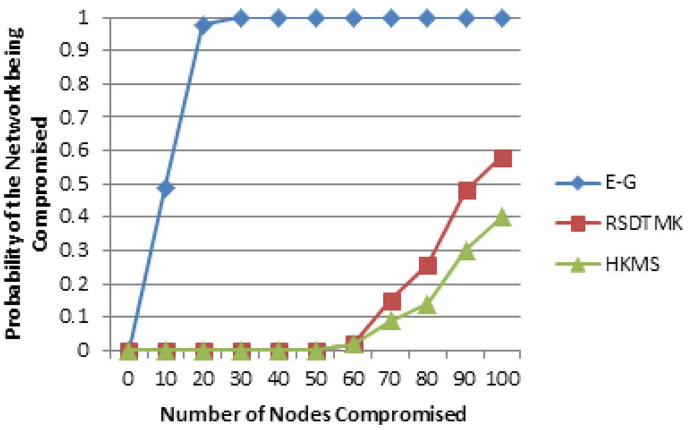

Fig. 6 Resilience analysis of HKMS with E–G and RSDTMK

5.3 Analysis of Energy Consumption for HKMS with E–G and RSDTMK

Energy consumption is referred to as the total quantities of energy drained by the nodes in the wireless sensor network to establish a common key by performing computation and broadcasting the key information related to the key establishment.

The decisive factor of communication consumption is the message's size being transmitted or broadcasted to form a key between sensor nodes. The energy consumed by each protocol to establish a shared key is shown in Fig. 7. The simulated results concluded that energy consumption for HKMS conserves30.67% of transmission energy compared to the existing E–G and RSDTMK scheme.

5.4 Comparison of Packet Broadcast Delay for HKMS with Existing Schemes

The broadcast delay is an important problem for critical event monitoring in WSNs. Figure 8 shows the broadcast delay of the sensor nodes in the network. The proposed protocol broadcast delay is 13.07% lesser than the existing scheme. It requires minimum time delay to establish a key between the neighbor nodes. Each node requires only broadcasting its identity during the key establishment phase. The proposed protocol reduces the time delay and the number of packets needed to communicate with neighboring sensor nodes for establishing a session key.

The proposed HKM scheme is compared with the E–G scheme [18] and RSDTMK Scheme [20] for the above-discussed metrics. The performance values are tabulated in Table 7. From Table 7, it is inferred that the performance of HKMS is better when compared to E–G and RSDTMK. The 100% of connectivity is achieved by proposed method as compared to the E–G and RSDTMK for key size of 10. The proposed Hybrid key management decreases the probability of link compromised between the sensor nodes by 9% than the existing scheme. The attacker has to capture more number of sensor nodes to compromise the link between the nodes. It provides more resilience against node capture attack even though the attacker knows the key-ring stored in the compromised node. The reconstruction of key pool is not possible because the key-rings are generated by one way

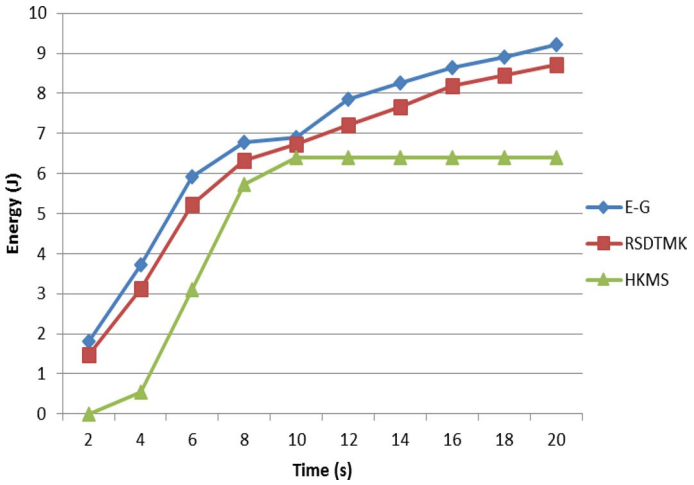

Fig. 7 Comparison of transmission energy consumption of HKMS with existing schemes

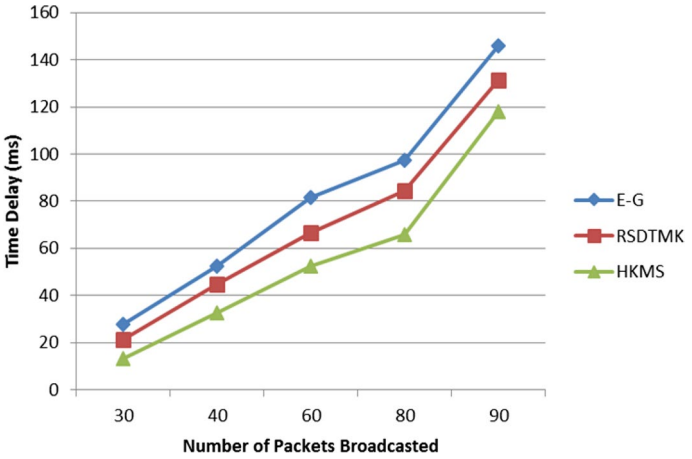

Fig. 8 Packet broadcast delay analysis of HKMS with E–G and RSDTMK

Table 7 Comparison of different techniques with respect to various parameters

Parameters	E–G	RSDTMK	HKMS
Connectivity for Key Ring Size (r = 10)	12%	80%	100%
Resilience with respect to Number of Node Compromised (70)	100%	15%	9%
Energy consumption	9.2 J	8.8 J	6.2 J
Packet broadcast delay	145 ms	128 ms	118 ms

hash function. The energy consumption for proposed hybrid key management is conserves 30.67% of transmission energy compared to the existing E–G and RSDTMK scheme due to less communication cost. The broadcast delay is 13.07% lesser than the existing scheme. It requires minimum time delay to establish a key between the neighbor nodes. Each node needs to broadcast only their identity during key establishment phase. The proposed protocol minimizes the time delay and number of packets need to communicate with neighbor sensor nodes to establish a session key.

6 Conclusions

In this paper, the edge nodes are deployed for key predistribution in Wireless sensor networks. The novel hybrid key management scheme for WSNs along with edge node to pre-distribute and establish the secure and authenticated communication link between the nodes using symmetric and asymmetric key cryptography has been proposed. The hybrid scheme incorporates the advantages of ECC based key pre-distribution scheme with a hash function and shared key between the nodes, which can be achieved by broadcasting the node's identity without sharing the key materials. The proposed Hybrid Key Management scheme conserves 30.67% of transmission energy and broadcast delay is 13.07% lesser than the existing scheme. The HKMS increases the connectivity and the probability of link compromise between the sensor nodes decreased by 39% than

the existing methods. The performance study of the proposed key management scheme shows that the link formation between the nodes increases, provides mutual authentication among the nodes, and resists against node capture attack compared to the basic E–G and RSDTMK scheme. However, to effectively reduce the latency to determine the rekeying material present at locally at edge or in cloud as well as to increase the lifetime of WSNs with less energy consumption, the WSNs necessitates the federated learning mechanism. Another promising direction for further extending the proposed method is to by implementing federated learning algorithm at edge node to aggregate the data receives from each sensor node and updates the global data to cloud.

Authors' Contributions All authors equally contributed in this work.

Funding Open Access funding enabled and organized by CAUL and its Member Institutions. No funds received to carry out this work.

Availability of Data and Material Data is available on request.

Code Availability Code is available on genuine request.

Declarations

Conflicts of Interest Authors have no conflict or competing interests.

References

1. Shahraki, A., Taherkordi, A., Haugen, Ø., & Eliassen, F. (2021). A survey and future directions on clustering: From WSNs to IoT and modern networking paradigms. *IEEE Transactions on Network and Service Management, 18*(2), 2242–2274. https://doi.org/10.1109/TNSM.2020.3035315
2. Ghosh, A., Shankar, B. U., Bruzzone, L., & Meher, S. K. (2010). Neuro-fuzzy-combiner: An effective multiple classifier system. *International Journal of Knowledge Engineering and Soft Data Paradigms, 2*(2), 107–129.
3. Sharmila, Kum Kum, Umang Kant, and Pramod Kumar, "Secure trust aware hybrid key management routing protocol for WSNs for the application of IoT". International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278–3075, Volume-8, Issue-9S4, July 2019.
4. Yuan, E., Wang, L., Cheng, S., Ao, N., & Guo, Q. (2020). A key management scheme based on pairing-free identity based digital signature algorithm for heterogeneous wireless sensor networks. *Sensors, 20*(6), 1543.
5. Zhang, Q., Li, Y., Zhang, Q., & Yuan, J. (2019). "A self-certifiedcross-cluster asymmetric group key agreement for WSNs. *Chinese Journal of Electronics, 28*(2), 280–287.
6. Kandris, D., Nakas, C., Vomvas, D., & Koulouras, G. (2020). Applications of wireless sensor networks: An up-to-date survey. *Applied System Innovation, 3*(1), 14.
7. Al-taha, M. A. (2018). Symmetric key management scheme for hierarchical wireless sensor networks. *International Journal of Network Security & Its Applications (IJNSA)*, *10*(3), 2018.

8. Hamsha, K., & Nagaraja, G. S. (2019). Threshold cryptography-based lightweight key management technique for hierarchical WSNs. *Ubiquitous Communications and Network Computing, 276*, 188–197.
9. Kumar, A., Bansal, N., & Pais, A. R. (2019). New key pre-distribution scheme based on combinatorial design for wireless sensor networks. *IET Communications, 13*(7), 892–897.
10. Sehwag Albakri, LeinHarn, Sejun Song, "Hierarchical key management scheme with probabilistic security in a wireless sensor network (WSN),"*Security and Communication Networks*, 2019. https://doi.org/10.1155/2019/3950129
11. Sharmila, R., Vijayalakshmi, V., & Rajashree, R. (2016). An energy-efficient routing protocol using hybrid evolutionary algorithm in wireless sensor networks. *International Journal of Knowledge Engineering and Soft Data Paradigms, 5*(3/4), 285–301.
12. Gautam, A. K., & Kumar, R. (2021). A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. *SN Appl. Sci., 3*, 50. https://doi.org/10.1007/s42452-020-04089-9
13. Bhushan, S., Kumar, M., Kumar, P., et al. (2021). FAJIT: A fuzzy-based data aggregation technique for energy efficiency in wireless sensor network. *Complex Intell. Syst., 7*, 997–1007. https://doi.org/10.1007/s40747-020-00258-w
14. Chen, C.-T., Lee, C.-C., & Lin, I.-C. (2020). Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments. *PLoSONE, 15*(4), e0232277.
15. Simplício, M. A., Jr., Barreto, P. S., Margi, C. B., & Carvalho, T. C. (2010). A survey on key management mechanisms for distributed wireless sensor networks. *Computer Networks, 54*(15), 2591–2612.
16. Ould Amara, S., Beghdad, R., & Oussalah, M. (2013). Securing wireless sensor networks: a survey. *EDPACS, 47*(2), 6–29.
17. Mehmood, G. (2021). "An efficient and secure session key management scheme in wireless sensor network." *Complexity*. https://doi.org/10.1155/2021/6577492
18. M. A. El Hafez Bakr, M. A. Mokhtar and A. El Sherbini Takieldeen, "Modified elliptic curve cryptography in wireless sensor networks security." In: 2018 28th International Conference on Computer Theory and Applications (ICCTA), 2018, pp. 13–18, https://doi.org/10.1109/ICCTA45985.2018.9499173
19. L. Eschenauer, and V.D.Gligor, "A key-management scheme for distributed sensor networks," *In: Proceedings of the 9th ACM Conference on Computer and Communications Security*, Washington, USA, Nov. 18–22, 2003. pp. 41–47.
20. R. Blom, "An optimal class of symmetric key generation systems", *Advances in Cryptology: Proc. EUROCRYPT '84*, Paris, France, December 1985, pp. 335- 338.
21. Gandino, F., Celozzi, C., & Rebaudengo, M. (2017). A key management scheme for mobile wireless sensor networks. *Applied Sciences, 7*(5), 490.
22. Gandino, F., Montrucchio, B., & Maurizio, R. (2014). Key management for static wireless sensor networks with node adding. *IEEE Transactions on Industrial Informatics, 10*(2), 1133–1143.
23. Shim, K.-A. (2017). BASIS: A practical multi-user broadcast authentication scheme in wireless sensor networks. *IEEE Transactions on Information Forensics and Security, 12*(7), 1545–1554. https://doi.org/10.1109/TIFS.2017.2668062
24. Moghadam, M. F., Nikooghadam, M., Jabban, M. A. B. A., Alishahi, M., Mortazavi, L., & Mohajerzadeh, A. (2020). An efficient authentication and key agreement scheme based on ECDH for wireless sensor network. *IEEE Access, 8*, 73182–73192. https://doi.org/10.1109/ACCESS.2020.2987764
25. Bhushan, Shashi, Anil Saroliya, and Vijander Singh. "Implementation and evaluation of wireless mesh networks on MANET routing protocols." *International Journal of Advanced Research in Computer and Communication Engineering* 26 (2013).
26. Adavoudi-Jolfaei, A., Ashouri-Talouki, M., & Aghili, S. F. (2019). Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks. *Peer-Peer Netw. Appl., 12*(1), 43–59.
27. Yousefpoor, M. S., & Barati, H. (2019). Dynamic key management algorithms in wireless sensor networks: A survey. *Computer Communications, 134*, 52–69.
28. Athmani, S., Bilami, A., & Boubiche, D. E. (2019). EDAK: An efficient dynamic authentication and key management mechanism for heterogeneous WSNs. *Future Gener. Comput. Syst., 92*, 789–799.
29. Nikooghadam, M., Jahantigh, R., & Arshad, H. (2017). A lightweight authentication and key agreement protocol preserving user anonymity. *Multimed Tools Appl, 76*, 13401–13423. https://doi.org/10.1007/s11042-016-3704-8
30. Seo, S.-H., Won, J., Sultana, S., & Bertino, E. (2015). Effective key management in dynamic wireless sensor networks. *IEEE Trans. Inf. Forensics Security, 10*(2), 371–383.
31. Kishore, R., Radha, S., & Rose, S. H. (2009). Improved key predistribution scheme in wireless sensor networks using cell splitting in hexagonal grid based deployment model. *International Journal of Distributed Sensor Networks, 5*(6), 850–866.

32. Gulen, U., & Baktir, S. (2020). Elliptic curve cryptography for wireless sensor networks using the number theoretic transform. *Sensors (Basel)., 20*(5), 1507. https://doi.org/10.3390/s20051507. PMID:32182915;PMCID:PMC7085706
33. Feroz Khan, A. B., & Anandharaj, G. (2021). A cognitive energy efficient and trusted routing model for the security of wireless sensor networks: CEMT. *Wireless Personal Communications, 119*, 3149–3159. https://doi.org/10.1007/s11277-021-08391-6
34. Feroz Khan, A. B., & Anandharaj, G. (2019). A cognitive key management technique for energy efficiency and scalability in securing the sensor nodes in the IoT environment: CKMT. *SN Appl. Sci., 1*, 1575. https://doi.org/10.1007/s42452-019-1628-4
35. Ishmanov, F., Malik, A. S., Kim, S. W., & Begalov, B. (2015). Trust management system in wireless sensor networks: Design considerations and research challenges. *Transactions on Emerging Telecommunications Technologies, 26*(2), 107–130.
36. Singh, A. K., Alshehri, M., Bhushan, S., Kumar, M., Alfarraj, O., & Pardarshani, K. R. (2021). Secure and energy efficient data transmission model for WSN. *Intelligent Automation and Soft Computing, 27*(3), 761–769.
37. Yousefpoor, M. S., & Barati, H. (2020). DSKMS: A dynamic smart key management system based on fuzzy logic in wireless sensor networks. *Wireless Networks, 26*(4), 2515–2535.
38. Chauhan, S., & Tyagi, S. B. (2014). Performance evaluation of reactive routing protocols In VANET. *International Journal of Innovations and Advancement in Computer Science, 3*(9), 189–193.
39. Ali, S., Humaria, A., Ramzan, M. S., Khan, I., Saqlain, S. M., Ghani, A., & Alzahrani, B. A. (2020). An efficient cryptographic technique using modified Diffie-Hellman in wireless sensor networks. *International journal of distributed sensor networks, 16*(6), 1550147720925772.
40. Apsara, M. B., Dayananda, P., & Sowmyarani, C. N. (2020). A review on secure group key management schemes for data gathering in wireless sensor networks. *Engineering, Technology & Applied Science Research, 10*(1), 5108–5112.
41. Gupta, S., Gupta, S., & Goyal, D. (2021). Comparison of Q-coverage P-connectivity sensor node scheduling heuristic between battery powered WSN & energy harvesting WSN. *International Journal of Sensors Wireless Communications and Control, 11*(5), 553–559.
42. Chithaluru, P. K., Khan, M. S., Kumar, M., & Stephan, T. (2021). ETH-LEACH: An energy enhanced threshold routing protocol for WSNs. *International Journal of Communication Systems, 34*(12), e4881.
43. Aggarwal, A., Alshehri, M., Kumar, M., Alfarraj, O., Sharma, P., & Pardasani, K. R. (2020). Landslide data analysis using various time-series forecasting models. *Computers & Electrical Engineering, 88*, 106858. https://doi.org/10.1016/j.compeleceng.2020.106858
44. Singh, A. K., Alshehri, M., Bhushan, S., Kumar, M., Alfarraj, O., & Pardarshani, K. R. (2021). An energy-efficient and secure data transmission model for WSN. *Intelligent Automation & Soft Computing, 25*(3), 761–769. https://doi.org/10.32604/iasc.2021.012806
45. Corcoran, P., & Datta, S. K. (2016). Mobile-edge computing and the internet of things for consumers: Extending cloud computing and services to the edge of the network. *IEEE Consumer Electronics Magazine, 5*(4), 73–74.
46. Zhao, Z., Min, G., Gao, W., Wu, Y., Duan, H., & Ni, Q. (2018). Deploying edge computing nodes for large-scale IoT: A diversity aware approach. *IEEE Internet of Things Journal, 5*(5), 3606–3614. https://doi.org/10.1109/JIOT.2018.2823498
47. Xu, Z., Cai, M., Li, X., Hu, T., & Song, Q. (2019). Edge-aided reliable data transmission for heterogeneous edge-IoT sensor networks. *Sensors, 19*(9), 2078.
48. Hu, Y. C., Patel, M., Sabella, D., Sprecher, N., & Young, V. (2015). Mobile edge computing a key technology towards 5g. *ETSI White Paper, 11*(11), 1–16.
49. Li, J., Wu, J., Chen, L., Li, J., & Lam, S. K. (2021). Blockchain-based secure key management for mobile edge computing. *IEEE Transactions on Mobile Computing, 22*(1), 100–114. https://doi.org/10.1109/TMC.2021.3068717
50. M.S.Yousefpoor and H. Barati, "Dynamic key management algorithms in wireless sensor networks: A survey," Computer Communications, 2018.
51. Messai, M.-L., & Seba, H. (2016). A survey of key management schemes in multi-phase wireless sensor networks. *Computer Networks, 105*, 60–74.
52. Wang, Y., Man, K. L., Lee, K., Hughes, D., Guan, S.-U., & Wong, P. (2020). Application of wireless sensor network based on hierarchical edge computing structure in rapid response system. *Electronics, 9*(7), 1176. https://doi.org/10.3390/electronics9071176

Dr. Sharmila is working as an Assistant Professor, Department of Electronics & Communication Engineering, Krishna Engineering College, Ghaziabad, India. Sharmila completed her PhD from the Pondicherry University (central University), Puducherry. She has more than 10 years of experience in teaching. Her research contributions are highly interdisciplinary, spanning a wide range in research area includes Wireless Sensor Networks, Digital image Processing, Cryptography and Information Security, Block chain; area in which she has published and presented a greater number of research papers and one book and chapters in other books, published by IET, and Springer.

Dr. Pramod Kumar is working as Professor, Head (CSE) & Dean (CSE & IT) in Krishna Engineering College (KIET Group), Ghaziabad since January 2018. He also served as Director of the Tula's Institute, Dehradun, Uttarakhand. He has more than 23 years of experience in academics. He has completed his Ph. D in Computer Science & Engineering in 2011, M. Tech (CSE) in 2006. He is a senior member of IEEE (SMIEEE) and Joint Secretary of IEEE U.P Section. He has published widely in International Journals and Conferences his research finding related to Computer Network, Internet of things (IoT) and Machine Learning. He has Authored/Co-Authored more than 50 research papers and several Chapters in edited books. He has supervised and co-supervised several M. Tech and Ph.D. students. He has organized more than 12 IEEE International Conference in India and abroad and all the research paper of these conferences are now available in IEEE Explore. He is the editor of two book. He has published three patents. He has conducted more than 15 Faculty Development Program in the collaboration of EICT, IIT Roorkee, EICT, IIT Kanpur and AKTU. Funding for the FDP, Conference/Seminar received from AICTE/UGC /AKTU and departmental funding of various students' projects received from DST &MEITY. He has conducted IEEE National workshop on Research Paper writing on 27 March 2017 and IEEE Women Symposium on 21 Feb 2016.

Dr. Shashi Bhushan is an Assistant Professor in University of Petroleum and Energy Studies. He received the B.E. from University of Rajasthan, India and M. Tech degree in computer science from the Amity University Rajasthan in 2013 and the Ph.D. degree in computer science and engineering from in 2020. He has held a 9 years of university level teaching experience in computer science. He has several patents in the area of IoT. He has had many published articles in IEEE, Springer. He has organized, technical member and publicity chair of several international conferences. Area of research include wireless sensor network, internet of things.

Dr. Manoj Kumar completed his Ph.D. from The Northcap University and M.Sc. (Information Security and Digital Forensics) from Technological University, Dublin Ireland in 2013. He received fully-funded scholarship for his M. Tech and M.Sc. program from Irish Government. Dr. Kumar has 12.5+ years of experience in research, teaching, and industry. He is currently working on the post of Associate Professor in the University of Wollongong in Dubai, UAE. Dr. Kumar has published over 125 articles in International refereed journals and conferences. Dr. Kumar specializations are in Cyber Security, Digital Image Processing, Machine Learning, IOT, Digital Forensics, Networks and Information Security.

Dr. Mamoun Alazab is an Associate Professor at the College of Engineering, IT and Environment at Charles Darwin University, Australia. He received his PhD degree in Computer Science from the Federation University of Australia, School of Science, Information Technology and Engineering. He is a cyber security researcher and practitioner with industry and academic experience. Alazab's research is multidisciplinary that focuses on cyber security and digital forensics of computer systems with a focus on cybercrime detection and prevention. He has more than 150 research papers in many international journals and conferences, such as IEEE transactions on Industrial Informatics, IEEE Transactions on Industry Applications, IEEE Transactions on Big Data, IEEE Transactions on Vehicular Technology, Computers & Security, and Future Generation Computing Systems. He delivered many invited and keynote speeches, 24 events in 2019 alone. He convened and chaired more than 50 conferences and workshops. He works closely with government and industry on many projects, including Northern Territory (NT) Department of Information and Corporate Services, IBM, Trend Micro, the Australian Federal Police (AFP), the Australian Communications and Media Authority (ACMA), Westpac, United Nations Office on Drugs and Crime (UNODC), and the Attorney General's Department. He is a Senior Member of the IEEE. He is the Founding chair of the IEEE Northern Territory (NT) Subsection.

Authors and Affiliations

Sharmila[1] · Pramod Kumar[2] · Shashi Bhushan[3] · Manoj Kumar[4,6] · Mamoun Alazab[5]

Sharmila
sharmila1ece@gmail.com

Pramod Kumar
pramodkumar.hod@krishnacollege.ac.in

Shashi Bhushan
tyagi_shashi@yahoo.com

Mamoun Alazab
alazab.m@ieee.org

[1] Department of Electronics and Communication Engineering, Krishna Engineering College, Ghaziabad, Uttar Pradesh, India

[2] Dean Academics, Glocal University, Saharanpur, Uttar Pradesh, India

[3] Department of Computer Science, Amity University Punjab, Mohali, India

[4] Faculty of Engineering and Information Sciences, University of Wollongong in Dubai, Dubai Knowledge Park, Dubai, UAE

[5] IT and Environment, Charles Darwin University, Darwin 0909, Australia

[6] MEU Research Unit, Faculty of Information Technology, Middle East University, Amman 11831, Jordon