Multi-stage Key Management Scheme for Cluster based WSN

R Vijaya Saraswathi [1], Dr. L Padma Sree [2], Dr. K Anuradha [3]

[1]Dept.of CSE, VNR VJIET, Hyderabad, India
[2]Dept. of ECE, VNR VJIET, Hyderabad, India
[3]Dept. of CSE, GRIET, Hyderabad, India

Abstract**:** Secured communication over the Wireless Sensor Network (WSN) is one of the prime concerns nowadays as the wireless communication medium suffers under a wide range of security threats. For establishing secured communication over WSN, literature has suggested the multi-level key management protocol, where each transmission is established based on the availability of secured key. This work develops a key management protocol, namely Multi stage key management (MSKM) protocol, for the secured communication over the clustered WSN. The entire protocol is implemented in three stages, such as pre-deployment, key generation and key authentication and verification. In the first stage, the nodes are provided with the identity, and then, the second stage uses the homomorphic encryption model, for generating the necessary key to the communication. Finally, a mathematical model is developed in this work with several factors, such as a hashing function, homomorphic encryption, dynamic passwords, profile sequence, random number and EX-OR functions. The proposed MSKM protocol establishes the secured communication over the WSN by authenticating the entities. The entire work is compared with several states of art techniques and evaluated based on several metrics. The proposed MSKM protocol achieved values of 0.122 kb, 0.929kb, 2.332 kb and 14.586 joules for the communication overhead, detection accuracy, key memory storage and energy respectively.

Keywords: WSN Secured Communication, Key Management, Key Authentication, Homomorphic Encryption.

1. Introduction

Wireless Sensor Network (WSN) is one of the commonly used platforms for wireless communication among vastly distributed sensors. WSN connects a large number of nodes in the wireless platform, as the nodes are distributed in thousands of kilometers from each other. The storage capacity of the nodes is generally low, and the computing power also fairly limited. The sensor nodes in the network are displaced to unattended places, and thus, controlled by one or more sink/gateway nodes [11]. Further, the WSN has an ad- hoc infrastructure-less platform. The sensor nodes in the WSN have its pressure, temperature, etc., and hence, the route established amidst them will have an adverse impact on each node. The communication among the sources is established as the multi-hop communication with the base station. The users prefer to use the WSN for long distance communication as it needs less power, and easy to maintain [6]. The WSN makes use of the multiple sink or gateway nodes for establishing communication in the large area. Due to its increased credibility, the WSN is preferred in domestic and surveillance systems, environmental monitoring, agriculture, healthcare, disaster management, military application, and sensor nodes, which include analog to digital converter, micro-controller, external memory, transceiver and power source [11]. Large WSN is computationally expensive to maintain, and to avoid this problem; a clustering technique is preferred in the WSN to group the sensor nodes to each other. Clustering of WSN allows distinct portioning of the areas and thus, makes the maintenance to be a lot easier [18].

Cluster-based communication is preferred nowadays. However, cluster-based communication adds extra overhead and burden on the Cluster Head (CH) [19] in dense network scenarios, which eventually introduce delay and hinders network performance [20]. They are ubiquitous and can be deployed for mission-critical applications, such as smart grid, smart purposes, health care, target monitoring, etc. During these applications small, low-cost sensor nodes should be deployed at large scale. The constraints of the sensor nodes in WSN concerning the resources make the communications between the sensor nodes, between the base station and sensor nodes and among all the sensor nodes is a challenging task. To ensure the confidentiality of the messages, the messages within WSN must be encrypted [8][12].

Several literature works have opted to derive a secure transmission platform for WSN by improving the robustness against the node attacks. Secure communication platform makes the transmission to be resistance against the node attacks. Node attacks are common in WSN, as the architecture is an open platform. Node attacks primarily steal the key used for communication and steal/alter the message. One of the major aims of WSN is to establish a secured communication in various adversary scenarios [16]. In recent years, the communication between the nodes in WSN is done through Key Management Scheme (KMS), where a key is established for secured communication. KMS establishes a secured communication service between the WSN nodes, by defining a set of mechanism [4, 7]. While performing the communication with the KMS, a secret key is established among the sensor nodes and the communication entities for secured communication. Also, the secret keys used in the KMS need to refresh constantly for the secured communication [29]. Further, to the secured communication, KMS [10] need to ensure secure generation, distribution, and storage of the various keys used in the communication. This may fail in adverse condition, such that the expensive exponential algorithms present in the key management only establishes the secured key rather than encrypting the messages [5]. Thus it is necessary to establish the encryption algorithm separately in the key management protocols. The encryption techniques used in the key management protocols fall into three categories, they are symmetric, asymmetric and hybrid techniques [17]. In [21], dynamic group management protocol has been implemented as the encryption scheme for the WSN. In [23-25], some of the

encryption protocols related to the key management services in WSN are discussed.

The primary intention of this research is to design and develop a dynamic key management protocol based on mutual and multi-level verification in clustered WSN. The proposed key management protocol involves three entities, such as CH, sensor node, and base station for the key management in the WSN. The overall procedure of the proposed protocol includes the following three stages, such as pre-deployment, key generation, and key authentication and verification. In the pre-deployment stage, the sensor nodes in the network are provided with the identity, and in the key generation stage, lightweight key generation based on homomorphic encryption is used to generate the keys. Finally, the key authentication and verification are done by deriving a mathematical model using a hashing function, homomorphic encryption, dynamic passwords, profile sequence, random number, and EX-OR functions. Thus, with the developed mathematical model for the key management, the proposed protocol authenticates the entities and thereby, provides a secure and dynamic key management in the clustered WSN.

The contributions of this work towards establishing the secured management tool in WSN are briefed as follows:

- Development of the Multi Stage key management MSKM protocol, for authorizing dynamic key management in the clustered WSN.
- A mathematical model is developed with the hash function, homomorphic encryption, dynamic passwords, profile sequence, random number, and EX-OR functions, for performing the key authentication and verification phase.

The structure of this paper is briefed as follows: Section 1 presents the introduction to the clustered WSN and secured key management for wireless communication. Section 2 surveys some of the conventional techniques, which have established a key management protocol in WSN. Section 3 depicts the network model of the clustered WSN, and Section 4 presents the brief description of the proposed MSKM protocol and the mathematical model for key authentication and verification phase. The simulation results achieved by the proposed MSKM protocol along with its other comparative performance over another state of art techniques are depicted in section 5, and section 6 concludes the paper.

2. Related Work

This section presents the survey of seven literature works developed for the key management in WSN. Qi Jiang *et al.* [1] presented the lightweight authentication and key agreement protocols using the Rabin cryptosystem module. The authentication phase in the key management requires more weightage, as the actual security is established in this phase. Since the model used the Rabin cryptosystem module; the scheme ensured security against all possible attacks. The scheme provided the lightweight authentication for the internet integrated WSN. In this work, the actual performance cannot be measured accurately, and the computation cost for the gateway of this model was found to be higher than the computational cost of the Das's protocol and Amin *et al.*'s protocol. Samir Athmani *et al.* [2] presented the Dynamic Authentication and Key Management Mechanism for the secured communication over the WSN. The scheme considered the local information for identifying the valid sensor nodes for the communication. This improved the energy efficiency and the memory of the WSN, but this method solves only the security problems introduced by the key distribution schemes and does not recognize the other security issues, such as replay attack, privileged insider attack, and so on. R.Vijaya Saraswathi *et al.* [3] presented the dynamic and probabilistic key management protocol by developing the flexible network arrangements for security related features. It uses the pair-wise and group key management protocols for the secured transmission. Further, it uses the bloom filter for access. The drawback of the Bloom filter is that one cannot remove existing items without rebuilding the entire filter. Also, it suffered from performance overhead. It cannot reserve space for growth. Pratusha Laxmi B and Chilambuchelvan A [5] proposed the Geographic Secured Routing (GSR) protocol for the WSN by incorporating the SH3 Algorithm. Although the protocol provides node and message authentication, the computation overhead was very low. The protocol provides improved performance in the packed environment and also ensured guaranteed packet delivery. This method had some drawbacks, such as high energy consumption, suffered from various attacks on sleep scheduling algorithms.

Priyanka and Mayank Dawe [7] presented the highly secure key management scheme by exploiting security related features present in the WSN. The scheme overcame the issues, such as high node density, neighbor influence factor during the security enhancement. The model failed to develop an adaptive technique for mitigating the neighbor influence factor. Hash-based pre-distribution utilized in this method bring some extra overhead regarding storage of hash function. Xinjiang Sun *et al.* [9] proposed the self-healing key management schemes by developing the broadcast authentication enhanced collusion resistance module. The scheme achieved enhanced security and thus, tolerates the effects occurring due to packet loss. The scheme achieved improved resource consumption rate. However, many of the security related issues related to WSN are not discussed here. The configurability of self-healing capability, the security performance, and the adaptive size of the sliding window under unreliable links were not discovered in this work. Purushothama B R and Arun Prakash Verma [8] presented the group key management technique for the security enhancement of the WSN module. The scheme was specifically designed for mitigating the attacks arriving from the outside environment. Even though the scheme had enough performance, it suffered from limited energy, memory, and power. In this method, every key held by the sensors must be changed during every rekeying, which adds computational burden on the users and group controllers. Also, there was a need for secure channels, which needs additional communication cost.

Shraddha Deshmukh *et al*. [26] introduced Certificateless-effective key management (CL-EKM) principle for secure communication in WSN portrayed by hub versatility. This method was valuable in memory execution, correspondence, vitality, and time. The drawback of this method is that the identity information no longer forms the entire public key, which means that the user's public key is not discoverable from only the user's identity string and the Key Generation Center (KGC)'s public key. Jaewoo Choi *et al.* [27] developed a location-based key management scheme for

WSNs, with special considerations of insider threats. To address the communication interference problem in location-dependent key management (LDK), he introduced a key revision process, which included the grid-based location information. If a packet drop attack affected, every packet forwarded through the sensor nodes SNs was dropped, and the network loses its function.

The challenges involved during the secured data communication over the WSN are depicted below:

- Securing the network communication represents one of the most important challenges in WSNs. Most researches are based on key management, which suffers from problems, such as probabilistic key distribution between high-speed network (HSN) and low-speed network (LSNs), non-scalability after deployment, mounting weakness against node compromise, lack of memory storage on resource-limited LSNs and high-communication overhead [2].
- Broadcast source authentication is a challenging topic in WSNs. This security service allows senders to broadcast messages to multiple receivers in a secure way [15]. Hence, ensuring secure access to sensitive information in a WSN remains a topic of ongoing research challenge, partly due to the wide range of potential attacks and attack vectors [13].
- Limitations such as processing, memory constraints, limited network capacity, scarce energy reserves, etc., in WSN make the security enhancement to be vulnerable [14].
- The key pre-distribution solutions cannot be applied to the large-scale WSN [3].
- Key transfer which is done prior before the communication can be challenging in the dynamic network [3].

3. A Network Model for Clustered WSN

The proposed methodology for designing the key management system for the WSN is briefed in this section, and its architecture is depicted in figure 1.

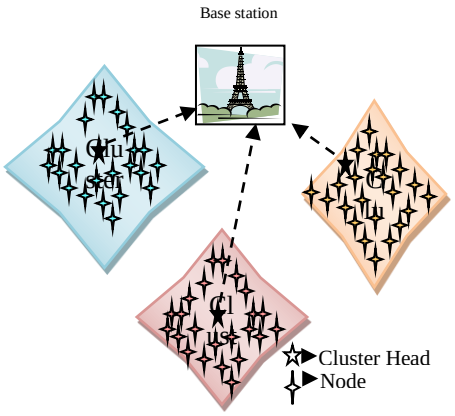

Figure 1. A Network Model of Clustered WSN

The clustered WSN initiates the data transfer after regulating the network with the CHs and routing protocol. The clustered WSN uses the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol for the cluster formation. The LEACH protocol is one among the commonly used protocols for selecting the CH among the group of nodes. The LEACH forms the cluster by considering the goal as 'the CH should consume minimal energy'. This criterion makes the clustering process more energy efficient. The LEACH protocol does the cluster formation at a simulation time **t**.

After certain duration of time, the energy of the CH will be reducing. Thus, the LEACH protocol will be simulated continuously in the given time interval **t**, for constantly selecting the CH.

The dynamic execution of the LEACH protocol in WSN mainly allows interruption and error-free communication service. After selecting the CH, the communication is carried between the nodes and Base Station (BS) via the selected CH. For establishing a secured communication link among the WSN, it is necessary to establish a communication link through a routing algorithm. The WSN nodes pass the information from one node to another through 'hopping'. Thus, the routing algorithm for the communication in clustered WSN is done with the multi-hop routing algorithm. The multi-hop routing algorithm finds the secured routing path between source and destination and transfers the data packets through the estimated routing path.

The clustered WSN has a total of P nodes, separated by indistinct distance. The nodes in the clustered WSN are represented as $\{n_1,n_2,K,.n_i,K,n_p\}$ and after the clustering process, the nodes are assigned to be CH, represented as $\{c_1,c_2,K,.c_k,K,c_H\}$ The nodes transfer the information from one node to other and finally, to the BS via the selected CH. The nodes send the message from sender to receiver, by encrypting the message with the secret key, and thus preserves the message authentication. The data packets sent from one node to another has three subfields, such as header, data, and code. Figure 2 represents the general structure of the message transferred between the nodes.

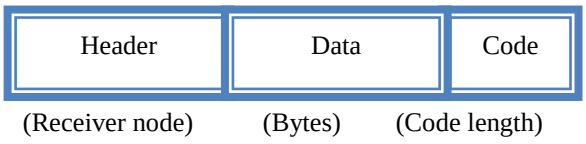

Figure 2. The General Format of the Message

4. Key Management for Clustered WSN with the Proposed MSKM Protocol

This section describes the proposed MSKM protocol, for establishing a secured communication link in clustered WSN. The proposed MSKM protocol performs key management in three different phases. The architecture of MSKM protocol is depicted in figure 3.

As presented in the above figure, the MSKM three phases are 1) Pre-Deployment, 2) Key Generation, and 3) Key Authentication and Verification phase. The proposed MSKM protocol can be considered as the improvement to the Goldwasser–Micali (GM) tool, such that the proposed MSKM protocol makes use of the public key for secure transmission.

The steps involved in the proposed MSKM protocol are briefed as follows:

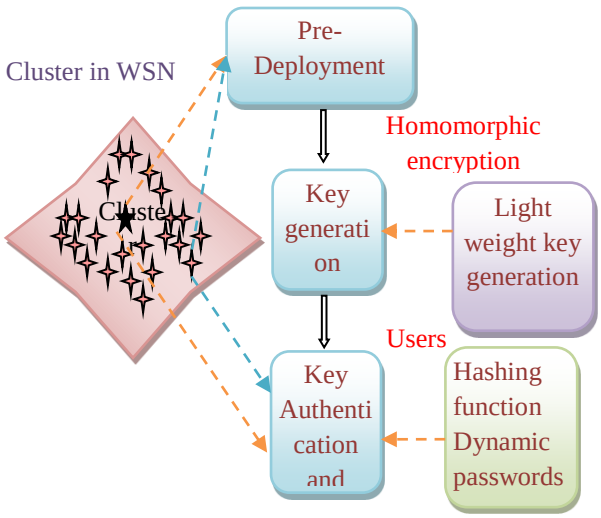

Figure 3. MSKM protocol in the dynamic cluster based WSN

A. Pre-Deployment Phase

The initial step in the proposed MSKM protocol is the pre-deployment phase, where the nodes are given a specific identity. Generally, the pre-deployment phase allocates the possible identification for each node, BS, and CHs. As the CH is one of the primary needs in WSN communication, the pre-deployment is done after the clustering of WSN nodes. After clustering the WSN, several CHs are formed.

The pre-deployment phase loads the predefined network key A_{key} to each node, CH and BS in the WSN. The WSN has its network parameter for each initiation of transmission. Most of the WSN use the network key of 128 bits for secured transmission. This paper adopts the homomorphic encryption [22] for generating the network key.

B. Key Generation phase

After providing the identity for the nodes, the next major phase is to generate key for an individual node, CH and BS. The key generation phase helps in generating the private and the public keys for the transmission amidst the nodes. This paper adopts the GM Encryption Scheme derived in [22] for generating the private and the public keys for the nodes. The steps adopted by GM scheme for key generation are explained as follows:

Consider the j^{th} node in WSN which initiates the transmission and it requires both the private key and the public key for the transmission purpose. Initially, the source node generates two distinct large prime numbers u and v. Then, the product Q = u.v is computed between the random numbers u and v. The nonresidue factor r is calculated as

$$r_u^{(u-1)/2} = -1(\mathrm{mod}\, u) r_v^{(v-1)/2} = -1(\mathrm{mod}\, v)$$

Public Key Generation: For generating the public key, the residual factor **r** and the product **Q** are used. Thus, the public key consists of **(r, Q)**.

Private Key generation: The private key is constructed based on **(u, v).**

The above steps are applied for generating the private and the public keys for the nodes, CH and BS. The key generated for nodes, CH and BS is given as follows:

For the node, $[N_{key}^R, N_{key}^U] = GM(u_1, v_1)$ (1)

For the CH, $[H_{key}^R, H_{key}^U] = GM(u_2, v_2)$ (2)

For the BS, $[B_{key}^R, B_{key}^U] = GM(u_3, v_3)$ (3)

Where, (u1,v1), (u2,v2) and (u3,v3) are set of large distinct prime numbers declared for the node, CH and BS, respectively.

C. Key Authentication and Verification phase

The final phase in the MSKM protocol is the authentication

The final phase in the MSKM protocol is the authentication and verification of the key. Figure 4 presents the flow of communication amidst the source and the destination node in the key authentication and verification phase. Before sending a secured message over the communication platform, it is necessary to establish a secured communication link between the nodes. The secured communication link is established between the sender and the receiver in the key authentication phase, before transferring the message. For each data transfer, the MSKM protocol generates the session key, for obtaining the cipher text.

Figure 4 states the operation flow during the authentication and verification phase. The data transfer gets initiates with the generation of the session key, and the transfer will be done once the secured communication link is established. The entire data flow done during the key authentication and verification phase is briefed as follows:

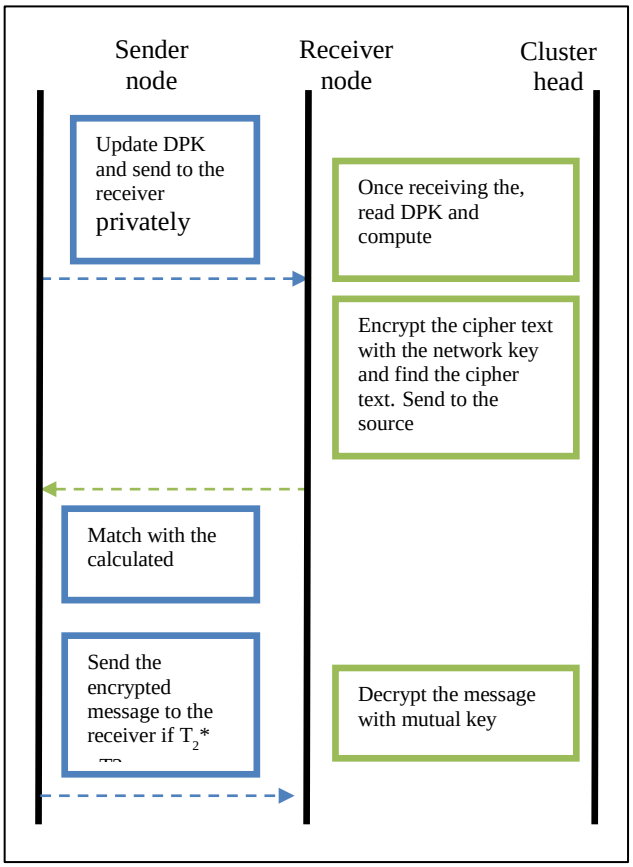

Figure 4. Key Authentication and Verification Phase of the Proposed MSKM Protocol

Initiate the data transfer: The message transfer is initiated by the source node and the message has its own identity, network key, and code. The message corresponding to the

nodes undergoes several changes to cope up with the security credentials. Consider the source node $\mathbf{n_i}$ initiates the data transfer to the destination node $\mathbf{n_j}$. Each node in the network maintains the dynamic profile key, which holds the information about the routing. The dynamic profile key used in the node is represented as DPK_{ij}. Here, i and j refer to the index of the source and destination nodes respectively. The dynamic profile key has the encrypted information about the message identity, receiver identity, along with the mutual key between nodes $\mathbf{n_i}$ and $\mathbf{n_j}$. The general format of the dynamic profile key is given as follows,

$$DPK_{ij} = \begin{bmatrix} E(Zid) & E(Rid) & E\left(W_{key}^{ij}\right) \\ M & M & M \end{bmatrix} \begin{matrix} Data_1 \\ Data_2 \\ M \\ Data_x \end{matrix} \quad (4)$$

where, Z_{id} indicates the message identity, R_{id} indicates the identity of the receiver node and W_{key}^{ij} refers to the mutual key generated between the source and the receiver. The function **E()** indicates the encryption, which is done using the existing GM algorithm with the help of the session key S_{key}^{+}. The session key is one of the important elements in the proposed MSKM protocol. The session key is generated temporarily, which lives for the communication session done during the data transfer between the node i and j. The following expressions indicate the encryption done through the GM scheme.

$$E[Z_{id}] = GM(Z_{id}, S_{key}^{+}) \quad (5)$$

$$E[R_{id}] = GM\left(R_{id}, S_{key}^{+}\right) \quad (6)$$

$$E[W_{key}^{ij}] = GM(W_{key}^{ij}, S_{key}^{+}) \quad (7)$$

Update DPK and send session key to the receiver privately: In the next step, the source updates the information and sends the session key to the receiver privately. The session key is retained until the end of the communication.

Compute the ciphertext T_1 at the receiver node: After attaining the session key from the sender, the receiver understands that the source is trying to communicate through the secured communication link. The MMKM protocol performs the data transfer only upon establishing the secured data link. For this type of communication, the receiver checks the validity of the source by generating ciphertext. Initially, the receiver generates the ciphertext $\boldsymbol{T_1}$. The ciphertext $\boldsymbol{T_1}$ is obtained based on the intermediate message I. The intermediate message I depends on the decrypted information with the session key, and it depends on the following equation,

$$I = \begin{bmatrix} D\left(E(Z_{id})|S_{key}^{+}(received)\right)||D \\ \left(E(R_{id})|S_{key}^{+}(received)|||D\left(E(Z_{id})|W_{key}^{ij}(received)\right)\right) \end{bmatrix} \quad (8)$$

Where, $S_{key}^{+}(received)$ refers to the session key received by the receiver, and D() indicates the decryption done on message entities based on the received session key. After the identification of the intermediate message I, the ciphertext T_i is identified by applying the hash function. The generation of ciphertext T_1 can be defined as follows,

$$T_1 = h(I) \quad (9)$$

Where, h() indicates the hash function. After performing the hashing operation over the intermediate message, the ciphertext T_1 is formed. Generation of ciphertext T_1 can be referred as the security layer 1.

Generate $\mathbf{T_2}$ and send to the source node: After establishing the first layer of security, the receiver creates the next layer of security by generating the ciphertext 2, referred to as T_2. The ciphertext T_2 is created based on the ciphertext T_1. The next layer of security is awarded by the network key, and thus, the ciphertext T_2 is generated as follows,

$$T_2 = \left[D\left(E(T_1)|A_{key}\right)||H_{key}^{u}\right] \quad (10)$$

where, A_{key} represents the network key. After generating T_2, the receiver responses the sender request by sending the ciphertext T_2. It is evident that the MSKM protocol acknowledges the message through multilevel security level, and thus, reduces the chance of security theft.

Compute T_2^* at the sender side: Once receiving the ciphertext T_2 from the receiver, the sender tries to decode the information. The sender initially constructs the intermediate message I* with message id, receiver id, and mutual key, and it is presented as follows,

$$I^* = \left[Z_{id}||R_{id}||W_{key}^{ij}\right] \quad (11)$$

where, I* refers to the intermediate information computed at the sender side. From this information, the sender reconstructs the ciphertext 1, indicated as T_1^*, and it is given as,

$$T_1^* = h(I^*) \quad (12)$$

where, T^*_1 indicates the ciphertext 1 constructed at the sender side. The reconstruction of ciphertext 1 is made possible by applying the hash function h(). Again, the sender finds the cipher text2, i.e. T_2^*, by applying the public key of the header node. The expression for formulating the T_2^* is referred as follows:

$$T_2^* = E\left(T_1^*|A_{key}||H_{key}^{u}\right) \quad (13)$$

After computing the ciphertext T_2^* in the sender side, this information can be used to validate the authenticity of the receiver node.

Match T_2 and T_2^* at the sender side: In this step, the actual message transfer occurs. The sender validates the authenticity of the receiver by matching the calculated ciphertext T_2^* with the ciphertext received from the receiver T_2. Once both the ciphertext matches, i.e. $T_2^* = T_2$, the sender declares the receiver to be valid and thus, initiates the original data transfer. If the cipher does not match, the communication will be terminated, and the session key generated for the communication gets expired.

Send the encrypted information to the receiver: After matching the ciphertext, the source sends the original message to the receiver by encrypting the message with the mutual key. The encrypted message sent to the receiver is depicted below:

$$E_{message} = E\left(Z|W_{key}^{ij}\right) \quad (14)$$

Decrypt the message at the receiver side: After receiving the encrypted message, the message received by the receiver is represented as $\boldsymbol{E_{message}(received)}$. Upon receiving the message, the information can be used by a receiver only through the decryption. The decryption done in the receiver node uses the mutual key and thus, can be represented as

$$\mathrm{Z(received)} = \mathrm{D}\big(\mathrm{E_{message}(received)}\big)|\mathrm{W_{key}^{ij}} \quad (15)$$

In the above stated MSKM protocol, it is ensured that the MSKM protocol performs multilevel security scheme for ensuring privacy among the nodes. In the existing works, either private or public key is used for ensuring security, but the proposed MSKM protocol uses both private and public keys for ensuring the security.

The operation flow for the key authentication and verification phase is depicted in algorithm 1.

Algorithm 1. Pseudo code of the proposed MSKM protocol

Sl.No	MSKM protocol
1	Parameters: nodes, CH, BS
2	//Pre-deployment phase
3	For each node, CH, BS
4	Find the network key A_{key} using GM algorithm
5	Assign the network key A_{key} to nodes, cluster head, BS
6	End for
7	//Key generation phase
8	For every node
9	Generate $[N_{key}^{R}, N_{key}^{U}]$ using GM algorithm
10	End for
11	For every CH
12	Generate $[H_{key}^{R}, H_{key}^{U}]$ using GM algorithm
13	End for
14	For BS
15	Generate $[B_{key}^{R}, B_{key}^{U}]$ using GM algorithm
16	End for
17	For every data sample
18	For j^{th} node in i^{th} cluster
19	Define the session key S_{key}^{+}
20	Perform encryption over the message identity, receiver identity, and mutual key
21	Assign $E[M_{id}] = GM(M_{id}, S_{key}^{+})$
22	Assign $E[R_{id}] = GM(R_{id}, S_{key}^{+})$
23	Assign $E[M_{key}^{ij}] = GM(M_{key}^{ij}, S_{key}^{+})$
24	//Key Authentication and Verification phase
25	Initiate the transmission
26	Source updates DPK and sends $S_{key}^{+}$to the receiver
27	The receiver computes the code message I using equation (8)
28	Compute the ciphertext T_1 using equation (9)
29	Compute the ciphertext T_2 using equation (10)
30	Source finds the code message I* using (11)
31	Source finds T_1* and T_2* using (12) and (13) respectively
32	If $(T_2^* = T_2)$
33	Initiate data transfer
34	Else
35	Declare the j^{th} node as the attacker
36	End for

5. Results and Discussion

This section presents the simulation results of the proposed MSKM protocol. The simulation results achieved by the proposed MSKM protocol are compared with several state of the art techniques defined in [1], [2] and [3], respectively. The performance of state of the art techniques is evaluated with the standard evaluation metrics.

a. Experimental Setup

The entire work of the MSKM protocol is implemented in the NS2 simulator, and further uses the PC with an Ubuntu OS, 4 GB RAM, and Intel I3 processor.

b. Simulation Setup

Simulation platform for the realization of MSKM protocol can be done by initializing the following parameters as depicted in table 1.

Table 1. Simulation parameters

Parameters in the simulation	Values
Simulation area A of the MANET	100 m X 100 m
Number of nodes in the MANET	100
The initial energy of the node	1 joule
The energy required to transmit the packet from the node	0.01 joule
The energy required to receive the packet from the node	0.01 joule
Mobility model	Random waypoint model
Size of the packet data	8 bytes

Here, the MSKM protocol is evaluated by two different scenarios, 1) With attack, and 2) Without attack. For the first type, simulation is done by introducing the selective packet drop attack, and Black Hole attack. In the second type of simulation platform, each node is free from all sorts of network attacks.

c. Performance Metrics

As the MSKM platform is specifically designed for secure transmission in WSN. Three metrics, such as key memory storage, communication overhead, and detection accuracy measure the effectiveness of the proposed MSKM protocol, and these metrics are given as follows,

Key memory storage: The key management protocols follow a key based service for communication in WSN, and as the WSN has limited memory, it is necessary to evaluate the memory requirement of the key. The key memory storage can be referred to as the size of the session key used for communication.

Communication overhead: Communication overhead occurs due to the non-availability of keys, and hence, the effect is limited to key deployment and generation phase.

Detection accuracy: The detection accuracy can be defined as the ratio of total attacks detected to the total number of attacks in the system.

$$\mathrm{DA} = \frac{\text{Attacks detected}}{\text{Total no of attacks}} \quad (16)$$

d. Comparative Techniques

The performance of the proposed MSKM protocol is compared with another state of art techniques, such as Efficient Dynamic Authentication and Key Management (EDAK) [2], three-factor [1], and probabilistic key [3]. The description of the comparative techniques is given as follows:

EDAK: The EDAK [2] technique employs the dynamic authentication criterion for providing the security to the WSN scheme. The scheme is limited to the heterogeneous WSN.
Three-factor authentication: In [1], a lightweight three-factor authentication scheme has been devised for the internet enabled WSN.
Probabilistic key: In [3], a probabilistic key management service was developed for resolving the issues present in large WSNs.

5.1 Comparative Analysis

Here, the comparative analysis is done by simulating the WSN platform subjected to three different conditions. They are, 1) Network facing the black hole attack [28], 2) Network facing the selective packet drop attack, and 3) Network without facing threats/ attacks. The evaluation of the proposed MSKM and other comparative techniques are done by varying the simulation time 't,' and the results are measured based on communication overhead, detection accuracy and key memory storage. For the improved performance, it is necessary to prove that the technique should achieve high detection accuracy along with low communication overhead and key memory storage.

5.1.1 Network under Black hole Attack

This analysis depicts the performance of the comparative techniques, while the nodes come under the scanner of black hole attack, and the graph is shown in figure 5.
Figure 5.a represents the analysis of the comparative model against the communication overhead metric, for the network that faces the black hole attack. For the time t= 50s, the comparative techniques, such as probabilistic key, three-factor, and EDAK techniques have the communication overhead of 0.500 kb, 0.566 kb and 0.625 kb respectively. For the same time, the proposed MSKM protocol achieved a low communication overhead value of 0.437 kb, which is 12.6%, 22.79% and 30.08% lower than the communication overhead of the existing methods. Further, the analysis depicts that the MSKM protocol outclassed other techniques by achieving low communication overhead during all runtime.
Figure 5.b represents the analysis of comparative models based on the detection accuracy metric, while the network is facing the black hole attack. For the time t= 50s, the comparative techniques, probabilistic key, three-factor and EDAK have the detection accuracy value of 0.578, 0.495 and 0.496. For the same time, the proposed MSKM protocol achieved high detection accuracy value of 0.614, which is 5.86%, 19.38% and 19.22% higher than the accuracy of the existing methods.
Figure 5.c represents the analysis of the comparative models based on the key memory storage metric, for the network facing the black hole attack. For the time t= 50s, the comparative techniques, probabilistic key, three-factor, and EDAK have the key memory storage value of 5.345 kb, 7.111 kb and 7.365 kb respectively. For the same time, the proposed MSKM protocol achieved low key memory storage value of 5.270 kb. The key memory storage of the proposed MSKM protocol is 1.41%, 25.89% and 28.45% lower than the key memory storage of the existing methods, probabilistic key, three-factor, and EDAK, respectively.
Figure 5.d shows the analysis of the comparative models based on energy for the network under black hole attack. For time t=50 sec, the energy of the proposed MSKM protocol is 12.289 joules, which is 1.78%, 5.32% and 5.05% higher than the energy of the existing techniques, probabilistic key, three-factor, and EDAK, respectively.

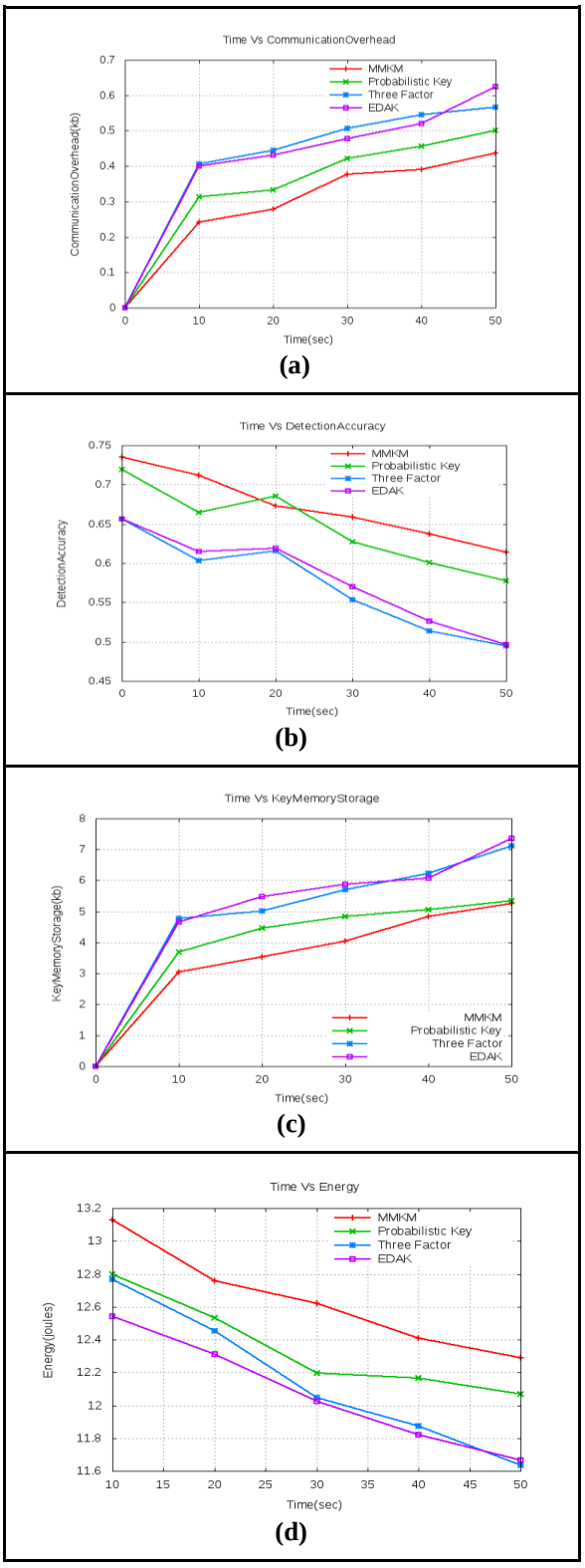

Figure 5. Analysis of comparative models for the network under a black hole attack based on (a) Communication Overhead, (b) Detection accuracy, and (c) Key Memory Storage (d) Energy Consumption.

5.1.2 Network under Selective Packet Drop Attack

This analysis depicts the performance of comparative techniques, for the nodes under the scanner of selective packet drop attack, and the graph is shown in Figure 6.

Figure 6.a presents the analysis of the comparative model against the communication overhead metric when the network faces the selective packet drop attack. For the time t= 50s, probabilistic key, three-factor, and EDAK techniques have the communication overhead value of 0.482 kb, 0.601 kb and 0.608 kb respectively. For the same time, the proposed MSKM protocol achieved a low communication overhead value of 0.454 kb, which is 5.81%, 24.46% and 25.33% lower than the communication overhead of the existing methods. Further, the analysis depicts that the MSKM protocol outclassed other techniques by achieving low communication overhead during all runtime.

Figure 6.b represents the analysis of comparative models based on the detection accuracy metric, for the network facing the selective packet drop attack. For the time t= 50s, the comparative techniques, probabilistic key, three-factor, and EDAK techniques have the detection accuracy value of 0.578, 0.468 and 0.489 respectively. For the same time, the proposed MSKM protocol achieved high detection accuracy value of 0.624, which shows 7.37%, 25% and 21.63% improvement than the existing methods.

Figure 6.c represents the analysis of comparative models based on the key memory storage metric, while the network is facing the selective packet drop attack. For the time t= 50s, the comparative techniques, probabilistic key, three-factor, and EDAK techniques have the key memory storage value of 5.596 kb, 7.188 kb and 7.118 kb. For the same time, the proposed MSKM protocol achieved low key memory storage value of 5.097 kb, which is 8.92%, 29.09% and 28.39% smaller than the key memory storage value of the existing methods. Figure 6.d shows the analysis of the comparative models based on energy for the network under selective packet drop attack. For time t=50 sec, the energy of the proposed MSKM protocol is 12.222 joules, which is 2.29%, 6.39% and 5.31% higher than the energy of the existing techniques, probabilistic key, three-factor, and EDAK, respectively.

5.1.3 Network without Attack

This analysis depicts the performance of comparative techniques when the nodes are not affected by attacks, and the graph is shown in figure 7. Figure 7.a represents the analysis of the comparative model against the communication overhead metric, while the network is without attack. For the time t= 50s, the comparative techniques, such as probabilistic key, three-factor, and EDAK techniques have the communication overhead value of 0.330 kb, 0.505 kb and 0.517 kb respectively. For the same time, the proposed MSKM protocol achieved a low communication overhead value of 0.285, which is 13.63%, 66.66% and 44.87% smaller than the communication overhead of the existing methods. Further, the analysis depicts that the MSKM protocol outclassed other techniques by achieving low communication overhead during all runtime.

Figure 7.b represents the analysis of comparative models based on the detection accuracy metric, while the network is without attack. For the time t= 50s, the comparative techniques, probabilistic key, three-factor, and EDAK techniques have the detection accuracy of 0.751, 0.720 and 0.712 respectively. Meanwhile, the proposed MSKM protocol achieved high detection accuracy value of 0.804, which is 6.59%, 10.45% and 11.44% higher than the accuracy of the existing methods, probabilistic key, three-factor, and EDAK.

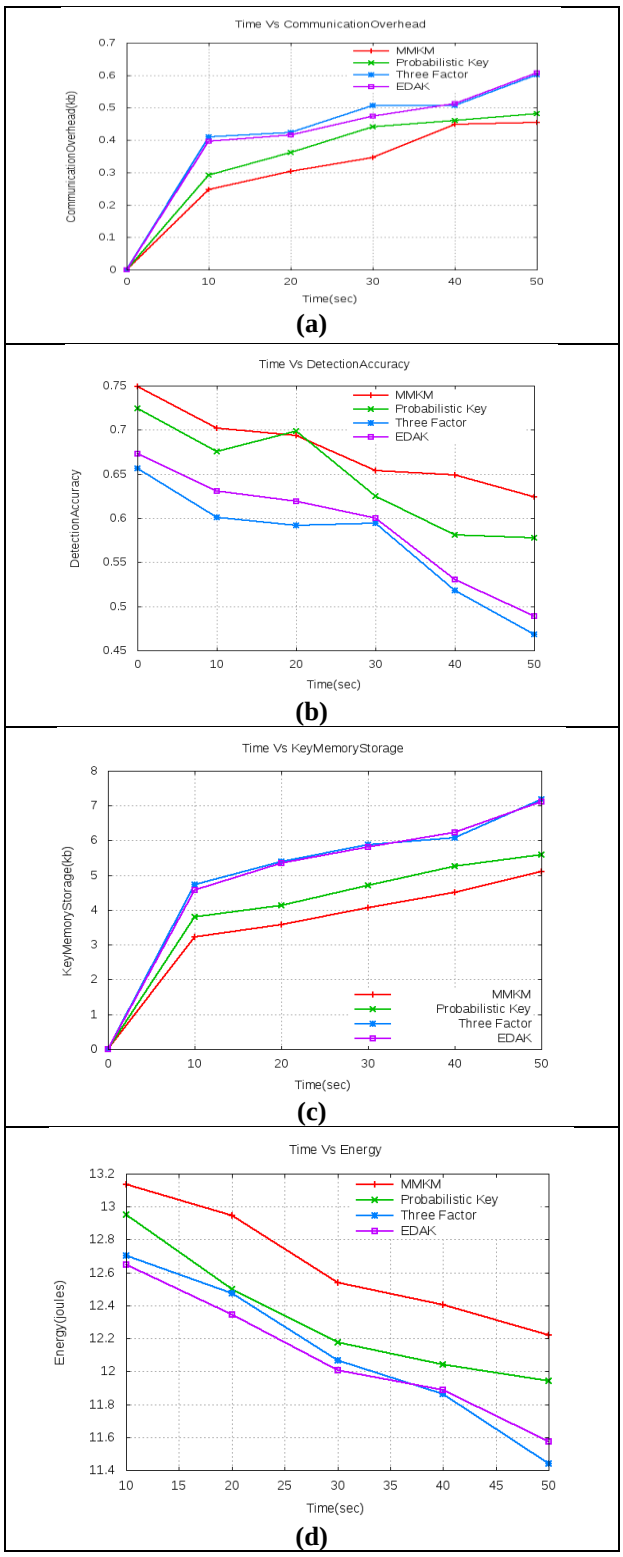

Figure 6. Analysis of Comparative Models for the network under Selective Packet drop attack based on (a) Communication Overhead, (b) Detection Accuracy, and (c) Key Memory Storage (d) Energy Consumption

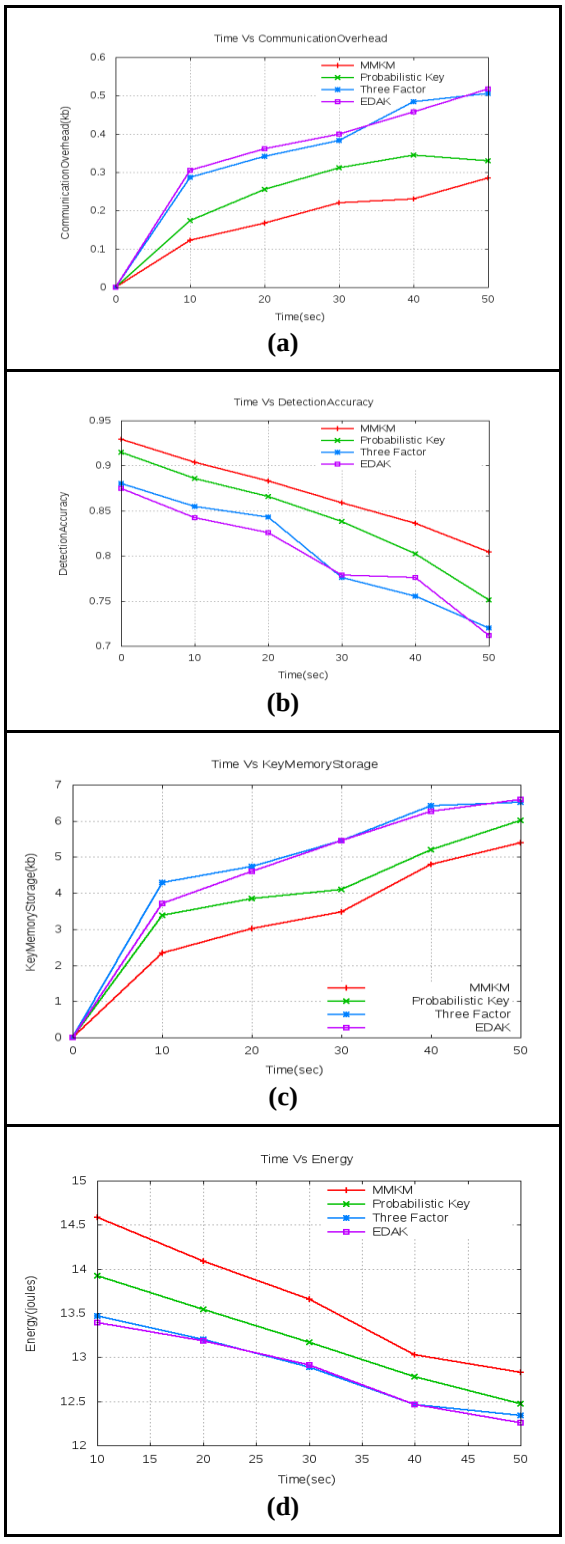

Figure 7. Analysis of comparative models for the network without attack based on (a) Communication overhead, (b) Detection accuracy, and (c) Key memory storage (d) Energy Consumption.

Figure 7.c represents the analysis of comparative models based on the key memory storage metric when the network is without attack. For the time t= 50s, the techniques, probabilistic key, three-factor, and EDAK techniques have the key memory storage value of 6.016 kb, 6.511 kb and 6.595 kb. For the same time, the proposed MSKM protocol achieved low key memory storage value of 5.396 kb, which is 10.31%, 17.12% and 18.18% smaller than the key memory storage value of the existing methods.

Figure 7.d shows the analysis of the comparative models based on energy for the network without attack. For time t=50 sec, the energy of the proposed MSKM protocol is 12.829 joules, which is 2.81%, 3.84% and 4.48% higher than the energy of the existing techniques, probabilistic key, three-factor and EDAK respectively.

5.2 Comparative Discussion

Simulation of environment is done with different attacks and without attack scenario shows that the proposed MSKM protocol outclassed other comparative techniques. Table 2 presents the comparative discussion of the performance of the techniques against the proposed MSKM protocol.

Table 2. Comparative Discussion for without Attack

Evaluation metrics	Comparative techniques			
	Probabilistic key	Three-factor authentication	EDAK	Proposed MSKM
Communication overhead	0.174	0.287	0.305	0.122
Detection accuracy	0.915	0.880	0.875	0.929
Key memory storage	3.384	4.301	3.722	2.332
Energy	13.925	13.469	13.389	14.586

Table 2 discusses the performance of the comparative model against the proposed MSKM protocol. The discussion suggests that the existing probabilistic key authentication scheme has the values of 0.174 kb, 0.915, 3.384 kb and 13.925 joules as the communication overhead, detection accuracy, key memory storage and energy respectively. The overall better performance is achieved by the proposed MSKM protocol, with the values of 0.122, 0.929, 2.332 and 14.586 as the communication overhead, detection accuracy and key memory storage.

Table 3 discusses the performance of the comparative model against the proposed MSKM protocol while the system is under attack. The discussion suggests that the existing three-factor authentication scheme has the values of 0.406, 0.656, 4.740 and 12.769 as the communication overhead, detection accuracy, key memory storage, and energy. The overall better performance is achieved by proposed MSKM protocol, with the values of 0.242 kb, 0.749, 3.059 kb and 13.137 joules as the communication overhead, detection accuracy, key memory storage and energy respectively.

Table 4 shows the key computation time of the proposed method and the existing methods. The existing methods, probabilistic key, three-factor, and EDAK have the key computation time of 8 sec, 8.5 sec and 7 sec respectively, while the proposed method has the minimum key computation time of 5 sec. From the analysis, it can be concluded that the proposed method provides the best performance in terms of communication overhead, detection accuracy, key memory storage and energy.The reason is that the proposed method develops the multilevel security link over the data communication to ensure the security. Also, that the proposed method utilizes the homomorphic encryption, which has a number of advantages, such as solve confidentiality problems, guaranteed privacy and so on.

Table 3. Comparative discussion for with attacks

Evaluation metrics	Comparative techniques			
	Probabilistic key	Three-factor authentication	EDAK	Proposed MSKM
Communication overhead	0.292	0.406	0.396	0.242
Detection accuracy	0.724	0.656	0.673	0.749
Key memory storage	3.698	4.740	4.580	3.059
Energy	12.950	12.769	12.648	13.137

Table 4. Key computation time of the comparative techniques

Methods	Key computation time (Sec)
Probabilistic key	8
Three-factor authentication	8.5
EDAK	7
Proposed MSKM	5

6. Conclusion

This work develops a key management protocol, namely MSKM, for the secured data transmission over the WSN. The proposed MSKM protocol establishes a secured communication link between the nodes and sends the encrypted information over the secured link. The proposed MSKM protocol ensures the security over the data communication by developing the multilevel security link. The MSKM protocol is specifically designed for the clustered WSN, and it has three stages, namely pre-deployment, key generation and key authentication and verification. The pre-deployment phase performs the identification task by providing the identity and the key to the nodes of WSN. In the next stage, homomorphic encryption is done for finding the encryption key. In the final stage, the mathematical model is developed with the secured factors, such as hashing function, homomorphic encryption, dynamic passwords, profile sequence, random number and EX-OR functions for secured data transmission. The entire work is compared with several states of art techniques and evaluated based on measures, such as memory, key storage, size, communication overhead and bandwidth utilization. Simulation results reveal that the proposed MSKM protocol achieved improved performance with the values of 0.122 kb, 0.929, 2.332 kb and 14.586 joules for the communication overhead, detection accuracy, key memory storage and energy respectively.

References

[1] Q. Jiang, S, Zeadally, J. Ma and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," in IEEE Access, vol. 5, pp. 3376-3392, 2017.

[2] Athmani, Samir, Azeddine Bilami, and Djallel Eddine Boubiche, "EDAK: An Efficient Dynamic Authentication and Key Management Mechanism for heterogeneous WSNs," in Future Generation Computer Systems, November 2017

[3] Saraswathi, R. Vijaya, L. Padma Sree, and K. Anuradha, "Dynamic and probabilistic key management for distributed wireless sensor networks," proceedings of IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-6, 2016.

[4] Azarderakhsh, Reza, Arash Reyhani-Masoleh, and Zine-Eddine Abid, "A key management scheme for cluster based wireless sensor networks," Proceedings of IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, vol. 2, pp. 222-227, 2008.

[5] Laxmi, B. Prathusha, and A. Chilambuchelvan. "GSR: Geographic Secured Routing using SHA-3 algorithm for node and message authentication in wireless sensor networks." in Future Generation Computer Systems, vol.76, pp 98-105, 2017

[6] Ramachandran, Shyamala, and Valli Shanmugam, "A two way authentication using bilinear mapping function for wireless sensor networks," in Computers & Electrical Engineering, vol.59, pp.242-249, 2017.

[7] Ahlawat, Priyanka, and Mayank Dave, "An attack model based highly secure key management scheme for wireless sensor networks," Procedia Computer Science, vol.125, pp. 201-207, 2018.

[8] B. R. Purushothama and A. P. Verma, "Security analysis of group key management schemes of wireless sensor network under active outsider adversary model," Proceedings of International Conference on Advances in Computing, Communications and Informatics, pp. 988-994, 2017.

[9] Sun, Xinjiang, Xiaobei Wu, Cheng Huang, Zhiliang Xu, and Jianlin Zhong, "Modified access polynomial based self-healing key management schemes with broadcast authentication and enhanced collusion resistance in wireless sensor networks," Ad Hoc Networks, vol.37 , pp.324-336, 2016.

[10] R Vijaya Saraswathi, L Padma Sree and K. Anuradha, "Key Management Schemes in Wireless Sensor Networks: A Survey" CiiT International Journal of Wireless Communication, Vol 8, No 05, May 2016.

[11] Srinivas, Jangirala, Sourav Mukhopadhyay, and Dheerendra Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," Ad Hoc Networks, vol. 54, pp. 147-169, 2017.

[12] Razaque, Abdul, and Syed S. Rizvi, "Secure data aggregation using access control and authentication for wireless sensor networks," Computers & Security, vol.70, pp. 532-545 2017.

[13] Amin, Ruhul, SK Hafizul Islam, Neeraj Kumar, and Kim-Kwang Raymond Choo, "An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks," in Journal of Network and Computer Applications, vol. 104, pp. 133-144, 2017.

[14] Challa, Sravani, Ashok Kumar Das, Vanga Odelu, Neeraj Kumar, Saru Kumari, Muhammad Khurram Khan, and Athanasios V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," Computers & Electrical Engineering, 2017.

[15] Chang, Shang-Ming, Shiuhpyng Shieh, Warren W. Lin, and Chih-Ming Hsieh, "An efficient broadcast authentication scheme in wireless sensor networks," in ACM Symposium on Information, computer and communications security, pp.311-320, 2006.

[16] He, X., Neidermeier, M., Meer, H, "Dynamic key management in wireless sensor network: a survey" in Journal of Network and Computer Applications, vol 36, pp. 612-622 2013.

[17] Zhang, J., Varadharajan, V ,"Wireless sensor network key management survey and taxonomy" Journal of Network and Computer Applications, vol.33, no.2, pp.63–75, 2010.

[18] Zahedi, Abdulhamid, "An efficient clustering method using weighting coefficients in homogeneous wireless sensor networks," in Alexandria Engineering Journal 2017

[19] Ouchitachen, Hicham, Abdellatif Hair, and Najlae Idrissi, "Improved multi-objective weighted clustering algorithm in

Wireless Sensor Network." Egyptian Informatics Journal, vol.18, no. 1, pp 45-54, 2017.

[20] Sharma, Sparsh, and Ajay Kaul, "Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET., Vehicular Communications, vol. 12, pp. 23-38, 2018.

[21] R Vijaya Saraswathi , L Padma Sree, and K Anuradha, "DynGKM: Dynamic Group Key Management Scheme for Cluster Based Wireless Sensor Networks," International Journal of Network Security, 2019.

[22] Xun Yi, Russell Paulet, Elisa Bertino, "Homomorphic Encryption and Applications," Springer Briefs in Computer Science, 2014

[23] Wu, Q., Mu, Y., Susilo, W., Qin, B. and Domingo-Ferrer, J., "Asymmetric group key agreement," In Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, Berlin, Heidelberg, pp. 153-170, 2009.

[24] Zhang, L., Wu, Q., Qin, B. and Domingo-Ferrer, J., "Identity-based authenticated asymmetric group key agreement protocol," In International Computing and Combinatorics Conference, Springer, Berlin, Heidelberg, pp. 510-519, 2010.

[25] Zheng, X., Huang, C.T. and Matthews, M., "Chinese remainder theorem based group key management," In Proceedings of the 45th annual southeast regional conference, pp. 266-271, 2007.

[26] Shraddha Deshmukh, Prof. A. R. Bhagat Patil, and Harshad Nakade, "Implementation of Effective Key Management Strategy with Secure Data Aggregation in Dynamic Wireless Sensor Network," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol.4, no. 2, pp. 358-364, 2018.

[27] Jaewoo Choi, Jihyun Bang, LeeHyung Kim, Mirim Ahn, and Taekyoung Kwon,"Location-Based Key Management Strong Against Insider Threats in Wireless Sensor Networks," IEEE Systems Journal, vol. 11, no. 2, pp. 494 - 502, June 2017.

[28] Houda Moudni , Mohamed Er-rouidi , Hicham Mouncifand Benachir El Hadadi, "Fuzzy Logic based Intrusion Detection System against Black Hole Attack in Mobile Ad Hoc Networks" International Journal of Communication Networks and Information Security (IJCNIS) Vol. 10, No. 2, August 2018.

[29] Reegan, A. Selva, and E. Baburaj, "Key management schemes in wireless sensor networks: a survey," Proceedings of International Conference on Circuits, Power and Computing Technologies, pp. 813-820, 2013.