International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Secure Hash Authentication and Cryptography Based Geographical Routing (SHAC-GR) for Wireless Sensor Networks

Manjunath D R, Thimmaraju S N

Abstract*: The expeditious growth in manufacturing anvils industries has lead towards the development of tiny devices. This growth has motivated to develop small and battery-operated sensor nodes that are widely adopted for establishing the reliable wireless communication. The wireless sensor based communication is generally divided into hierarchal and geographical deployment. Hierarchical system based approaches are widely studied in this field, limited work is present in the field of geographical WSN. In this work, we focus on the geographical WSN. Generally, these networks suffer from energy efficiency and security related issues. Hence, in this work we preset a combined approach to address these challenges. In order to mitigate the energy sparsity issue, we develop geographical routing scheme which selects the neighboring node based on residual energy of the node and distance from the sink node i.e. the maximum residual energy node from the neighboring node which is having less distance from the sink node is selected as next-hop. Due to this approach, the path computation and other network parameters computation is not required hence it reduces the power consumption. Further, we address the security issues where we present Hash modeling to secure the location, Key Exchange model for authentication by using ECDH approach , later we present ECIS based encapsulation method for data security and finally, a trust model based security system is developed. The trust computation of node helps to the routing whether to select the node for next hop or not. This multistage security approach is called as Secure Hash, Authentication and Cryptography based geographical routing (SHAC-GR) protocol. The proposed approach is simulated using MATLAB simulation tool and the performance of proposed approach is compared with existing technique that shows that the proposed approach improves the network performance in terms of network lifetime, energy and packet delivery rate.

***Index Terms*: Geographical Routing, Networks Security, WSN, Key Exchange, Energy Optimization.**

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Manjunath D R, Research scholar, Visvesvaraya Technological University, Belagavi.
Dr. Thimmaraju S N, Professor, Dept. of Masters of Computer Applications, Visvesvaraya Technological University, Centre for Post Graduate Studies, Mysore l.

I. INTRODUCTION

The recent growth in VLSI industries has enabled the evolution of small and tiny devices. This technological growth facilitates the development of small, battery-operated sensor nodes which leads towards the empowering the wireless communication using sensor nodes [1]. These sensor nodes are described according to their several characteristics such as low-cost for manufacturing, limited communication range, limited power supply capacity, and scarce computational capacities. Moreover, these sensor networks are equipped with the sensing circuitry that helps to detect and monitor a wide range of physical activities [2]-[3]. Due to these characteristics, sensor nodes are widely adopted in the various real-time application by forming a wireless sensor network that can deliver the desired monitoring for the considered region. Wireless Sensor Networks (WSNs) are formed by collaborating several sensor nodes, which are densely deployed in a random network region where these sensor node uses air as the medium to establish the communication among sensor nodes.

Despite of several promising applications of WSN, these networks suffer from several constraints and limitations of sensor nodes that are limited battery power, which affects the network lifetime performance. On the other hand, the network security is also considered as a challenging task, which can affect the network performance, monitoring and network reliability. However, several approaches have been introduced to address the network lifetime issue in WSNs[7]. In general, the energy consumption performance can be improved with the help of energy-aware routing protocols, based on this assumption, several researches are presented such as DEARER [4], TERP [5] and ETARP [6] etc.

On other hand, these routing schemes suffer from security related issues during communication process that is a crucial task due to the use of senor nodes in military and monitoring purpose that are the leading applications of WSN. In these application conditions, networks urge for confidentiality, integrity, authentication, data availability, data freshness and network scalability for developing a reliable communication model. if these issues are not addressed abruptly then it may challenge the data reliability and cause serious issues in network security. The sensor networks based communication systems contains several communication layers, which are more vulnerable to the security threats [8]-[9].

During last decade, several techniques have been introduced to mitigate the aforementioned challenges of network lifetime management and security in WSN. Elhoseny et al. [10] presented cryptography based scheme for secure WSN communication, ActiveTrust [11] using trust based mechanism, and key management scheme [12] for providing the efficient and secure communication. Some of the researches have focused on the
combined approaches to improve the network lifetime
by energy management and security such as ETARP [6], SGOR [13] and CASER [14] etc… Security is considered as a challenging task and less works are available for securing the WSN [15].

The performance of WSN depends on the routing that helps to deliver the packet to the destination node using multi-hop communication strategy. The routing protocols are mainly classified as Data-Centric protocol, Hierarchal protocol and location based protocol (Geographical routing) [16]. Data centric and hierarchal protocols have been studied by researchers and several promising solutions are introduced [17] whereas geographical routing protocols poses several challenges such as location privacy management and energy aware communication. Thus, here we mainly focus on the geographical routing in WSN.

Geographical routing based schemes are widely adopted in various real-time applications of WSN. The main aim of this approach is to provide the significant communication performance. Despite of efficient message delivery, energy management and QoS (Quality of Service) developing end-to-end secure communication is also a crucial task. Thus, secure routing development can be helpful in this scenario which can guarantee several security parameters such as confidentiality, authenticity, and data integrity etc. Similarly, reduced complexity in secured routing also can help to improve the performance of system. In these routing mechanisms, location privacy, key-management for authentication and data encryption-decryption are considered as important parameters which are responsible for security provisioning in the WSN. Thus, developing an end-to end location based secure routing approach is a main motivation of this work which can address the different types of security attacks.

The main contributions of the proposed work are as follows:

- Implementation of Hash based location privacy approach to secure the geographical location information of nodes.
- Implementation of ECDH based key exchange protocol to include the authentication of next hop
- ECIES-KEM based encapsulation method to perform the data encryption

Implementation of trust based model to include the new node and selecting the next hop from the deployed nodes.

II. RELATED WORKS

In this work, we present a brief discussion about recent techniques for security in WSNs. The recent advancements shows a significant improvement in wireless sensor network based communication. In this field of WSN, routing plays important role which has a significant impact on network performance. Several types of routing preset in the literature such as Data centric routing [19-20], hierarchical routing [21], and location based routing [22] etc…In this work, our main aim is to study about geographical or location based routing approaches for securing and improving the performance of WSN communication.

Wang et al. et al. [23] discussed about wireless multi-media sensor network, these networks takes advantages of different types of multimedia devices to monitor the environmental conditions. Due to use of multimedia data, meeting the requirement of QoS and delay reduction are the important and challenging tasks in WMSN. In this context, Multipath routing schemes shows a significant improvement that helps to utilize the resources and provides the efficient bandwidth for multimedia applications. The multipath routing schemes can improve the performance of WMSN when compared against the conventional routing protocols. However, the multipath routing suffers from the various issues such as data reliability, fault tolerance, bandwidth utilization, load balancing, and interference in geographical networks. In order to overcome these issue, based on direction geographical routing (DGR) a new approach is presented which uses pair-wise nodes around the sink and uses 360° path angle information. Moreover, energy consumption optimization is also incorporated during selection of next-hop, this process helps to balance the energy during entire communication. However, this techniques helps to achieve the better performance but mobility and node density is still considered a challenging task.

In [14] Tang et al. focused on energy management for lifetime improvement and security of WSNs. According to this process, energy balance control (EBC) routing is developed where average remaining energy of adjacent node is computed in the neighbouring grids and based on the maximum energy, the next hop is selected for routing. Thus, the message is transmitted to the grid where the next hop is closest to the destination node. At the same time, security level parameter is introduced which performs message forwarding and secure routing grid selection for communication. The security level parameter is used for selecting the secured path and message forwarding nodes. Thus, this approach is useful for providing the security and network lifetime improvement in WSNs.

Generally, internal attacks in sensor networks also degrades the performance of WSN communication. For this type of issues, trust and reputation management schemes show a significant impact on the security of WSN. Based on this assumption, Vamsi et al. [15] developed trust and location aware based secure routing called as TLAR approach. This approach is mainly divided into two stages where first of all trust is computed and then routing scheme is applied for data transmission. At the trust computation stage, direct and indirect consolidated trust values are computed and a trust metric is maintained.

Later, geographical routing is implemented using GPSR protocol where greedy and perimeter mode communication are used for constructing the routing path for successful data transmission.

Muthusenthil et al. [25] proposed privacy preserving scheme for MANETs by using cluster based geographical routing scheme. In any clustering technique, the cluster head formation is considered as an important task. In this work also, authors presented a novel approach for cluster head selection using node value that is computed using node mobility, degree of difference and residual energy. Once the cluster heads are formed, a group signature management scheme is developed which uses signature verification system to maintain the user authenticity. Finally, a packet routing scheme is developed for data transmission. Similarly, Thevar et al. [27] developed key management authentication scheme for secure WSN communication. In static WSNs the position of sensor nodes do not vary but in dynamic network environments, the node position varies over the time where nodes can be attacked and the performance of network can be degraded. In this types of scenarios, a particular node can be captured by the attackers which is called as captured node. To overcome this issue, authors present a key management based approach that helps to identify the neighbouring node and later node grouping and group head models are presented. In this approach, angular movement aware key management scheme is developed where mobile sensor nodes are considered as participating nodes and a secure key is established among these mobile nodes. Later, group authentication for security management is also developed to improve the performance.

The geographical routing shows significant impact in WSN and MANET networks. Recently, Punitha et al. [26] developed geographical routing based scheme for secure VANETs (Vehicular Ad-Hoc Networks) communication. The VANET follows dynamic topology which makes it more vulnerable to the security attacks where false information can be transmitted to the other neighbouring nodes. Hence, there is a need to develop a secure communication protocol which can provide trustworthy information that can help to improve the safety application in VANET scenario. However, several techniques are present for secure VANET communication but high speed, unstable connectivity and varying geographical locations poses several challenges that can degrade the network performance. In order to overcome these issues, a Privacy Preservation and Authentication on Secure Geographical Routing Protocol (PPASGR) is developed for VANET security. According to this process, the malicious nodes are identified with the help of forward and backward direction of antennas. Trusted Neighbour location is identified based on the trusted neighbouring table based location verification scheme which is obtained after Vehicle Tamper Proof Device (VTPD), and Trusted Authority (TA). The VTPD and TA generates the anonymous credentials for all vehicles.

Similarly, in [28] Zaimi et al. proposed a fuzzy logic based geographical routing for VANET communication. This approach mainly focuses on the QoS enhancement routing for multimedia data transmission. Hence, greedy perimeter

Stateless routing (GPSR) is considered as a base routing protocol and combined with the Fuzzy Logic approach. In this approach, fuzzy logic rules are generated based on the buffer size, delay and throughput parameters and based on the generated fuzzy rules, the best solution for next-hop selection is presented..

III. PROPOSED MODEL

In previous sections, we have studied about the advantages, application and challenges in the geographical routing. Literature review study shows that several techniques are present to improve the overall communication performance of Geographical networks. In this work, our main aim is to improve the communication performance of WSN using Geographical routing and address the security challenges. This section presents a complete model to improve the QoS and communication security in WSN which are deployed in geographical region. The complete proposed model is divided in to multiple stages where we present energy efficiency improvement and security management scheme.

A. Geographical Routing Protocol

For communication, wired networks make use of routers, and computationally efficient devices which are designed for forwarding the message to the destination. In these types of networks, the network topology is stable, moreover, the positions and configurations of nodes also do not change frequently. In contrast to this, sensor networks do not use any specific devices for routing the messages and each node participates to forward the message from source to destination node. Moreover, these networks are more dynamic and network topology changes over the time. Thus, the conventional approaches of wired network fails for the wireless sensor networks. To overcome these issues of WSN, three different type of routing protocols are introduced for WSN which are: proactive, reactive and Geographic Routing protocols. Proactive and reactive routing protocols are called topology-based protocols whereas Geographical routing protocols are called as location-based routing protocols. According to the proactive routing protocol, a complete information about network is maintained and frequent updates are propagated due to variations in network topology. Similarly, reactive protocols identify the new routes based on the communication demand with the help of flooding. However, these types of routing protocols violates the network bandwidth constraints and require more memory storage [29][30][31].

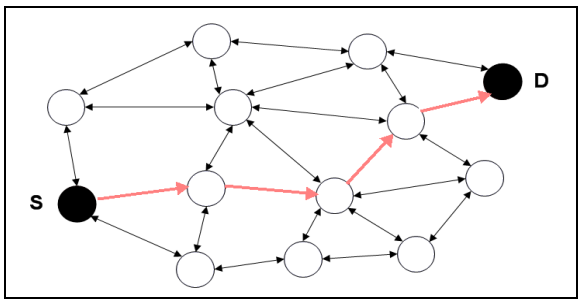

Fig 1. Geographical routing model

Beside these protocols, geographical routing protocols are introduced where geographical positions of nodes are considered to make the forwarding decisions. In these type of configuration, each node of the network knows their own positions and its neighboring nodes positions which can be obtained using broadcast message. The main advantages of this approach are: it requires very less routing information because all decisions are made based on the neighboring nodes, computation overhead, energy and computation time is reduced because of less
computation for route discovery. Memory requirement for each node is reduced because it requires very less information regarding the network topology. Due to these significant advantages, the Geographical routing is most suitable approach for lightweight sensor network application. A basic model of geographical routing is presented in figure 1.

In order to formulate the geographical routing, let us consider that a network graph G is presented as $G = (\mathcal{V}, \mathcal{E})$ where $\mathcal{N}$ number of sensor nodes are deployed in a geographic region. According to the geographical routing, a data packet is transmitted from source node $S \in \mathcal{V}$ to destination node $D \in \mathcal{V}$ by sending the packets over network edges and follows the conditions mentioned below:

- Each node in the sensor network knows their own and neighbouring node's geographical position in the network G
- The source node S has the position information about the destination node D
- Node is not allowed to store any information except the information about the next forwarding node.

In this work, we focus on the development of energy aware and secure geographical routing for wireless sensor networks.

B. Network Components

In this section, we present a brief discussion about network components, which are participating in the geographical network deployment which are deployed on a plane. Let us consider that each node n has geographical location coordinates as $L(n) = (n_x, n_y)$. The each node is equipped with the secured public key $\mathcal{K}_n$ that is used for encrypting the message m as $\mathcal{K}_p(m)$ and transmitted to the destination node. Similarly, each node n contains a private key PK_n that is only known to the node n. This private key cannot be computed using $\mathcal{K}_n$.

In this work we consider both malicious and faulty nodes for analysis where malicious nodes are responsible to provide the incorrect information whereas faulty nodes can be attacked and compromised to affect the information or network performance parameters.

New	Representation
$\mathcal{G}$	Euclidean graph
$\mathcal{V}$	Vertices
$\mathcal{E}$	Network edges
$\mathcal{N}$	Number of sensor nodes
L	Location
n	Each node
m	message
$\mathcal{K}_n$	Public key
PK_n	Private Key
p	Prime number
$\mathbb{I}$	Neighbour information list
$\mathbb{G}$	Geographical Hash

Similar to the faulty and malicious node, honest nodes are also present in the network which are identified based on their characteristics such as: these nodes are aware of accurate geographical location of sensor nodes, has the maximum range and efficiently perform the desired computation according to the proposed model. In this process the different types of sensor nodes such as faulty, malicious and honest nodes are deployed randomly and depending on their geographical location, these nodes participate in the communication where each nodes transmits the packets towards the destination node if the node is an honest node otherwise the packets can be dropped or altered before transmitting to the next hop. If any node does not have the one-hop neighborhood of the target location then the failure message is returned.

In this work, secure data transmission is our main concern where the data packets are transmitted through the secure path. The secure path is formulated with the help of combination of honest nodes. This routing protocol enables to identify the secure routing path to the destination where a neighboring honest node is identified near the desired geographical location. Once the next-hop node is identified, a secured message is returned as response, which contains the public key and secured path for communication. The next hop is obtained using proposed geographic routing approach and the response message is received at the source node using reverse path to the source node.

C. Attacks model in Geographical routing

In this section we discuss about the attacks which are handled by the proposed routing protocol. Several types of attacks are present which can attack on the data and node both. These type of attacks include message dropping, man in the middle, payload modification, and false location. The attacks on routed data consider payload or control data modification which can be used for identifying the operations of routing protocol. Similarly, the sensor nodes are also vulnerable to the attacks where sensor nodes can be compromised which can lead towards the malicious behavior of the node. Due to these malicious nodes, the compromised nodes can be used for continuously monitoring the location of the node causing the location privacy violations in the node.

In this work, we have focused on different types of attacks which can affect the routed data and the nodes. First of all, we focus on the node location privacy which is achieved using Hash function where each node ID and location information are stored in the form of Hash function. In the next phase, we aim on the reliable and stable communication establishment which is obtained using Key Exchange protocols, this also helps to overcome the man in the middle attack. For key generation, we make use of hybrid of ECC (Elliptic Curve Cryptography) and DSA (Digital Signature Algorithm) which provides public and private keys for each node. However, these keys are generated by each node. The key exchange part plays important role, if the key exchange is done successfully then the packet transmission can take place and a secure communication can be established. In contrast to this, during routing the data information can be attacked and the information can be leaked. Thus, we present a cryptography scheme where data can be encrypted and decrypted using generated public and private keys.

D. Proposed Key management, Trust computation hybrid Encryption scheme for WSN routing

Here we present the proposed solution for securing the WSN communication in geographical routing. The proposed approach is derived into multiple stages, which are as follows: first of all, we present a Hash Function based Model for encoding the geographical location information of each node.

A. Location Encoding using Hash Function

In this section, we present the Hash function based approach to encode the geographical location of sensor nodes. With the help of this, the sensor node maintains integer tokens where geographical locations are secretly associated. The geographical hash values are temporary which relies on the node location, as the node moves, the hash value of node also changes. Thus the hash values are computed repeatedly. In this work, we term this hash function generation as secure Hash.

Let us consider a large valued prime number denoted as p and a generating number g which can be used for mapping the set of prime numbers as $\mathbb{Z}_p^* = \{1, \dots, p-1\}$ with the help of a function $f(x) = g^x mod\ p$. In this, the each integer of $\mathbb{S}$ expressed as $h \in \mathbb{S}_p^*$ can be used for represet the one-way Hash function as $\mathcal{H}(x) = (g^h)^x\ mod\ p$. Finding the x in a given $y = g^x\ mod\ p$ is considered as NP-Hard problem. Let us consider that a sensor node $\mathcal{S}$ is repeatedly computing the secure Hashes using prime number p, generator g for prime number integer set $\mathbb{S}_p^* = \{1, \dots, p-1\}$ along with three integers as $\alpha_{\mathcal{S}}, \beta_{\mathcal{S}}, \gamma_{\mathcal{S}} \in \mathbb{S}_p^*$ and also a time interval indicator which represents the expiry time of the current secure Hash. The generation of secure hash is initialized as $(r_{\mathcal{S}}, r_{\mathcal{S}})$ at $\mathcal{S}$ where $r_{\mathcal{S}}$ denotes a randomly selected integer by node $\mathcal{S}$. The successive integers of $r_{\mathcal{S}}$ satisfy:

$$r_{\mathcal{S}}[i+1]\, g^{\theta_{\mathcal{S}}}\ mod\ p = r_{\mathcal{S}}[i] \quad (1)$$

With the help of these assumption, the secure Hashes of $\mathcal{S}$ at $\mathcal{S}_1$ as:

$$SH(\mathcal{S}, \mathcal{S}_1) = \left(r_{\mathcal{S}}\, g^{\alpha_{\mathcal{S}} \Delta x}\ mod\ p, r_{\mathcal{S}}\, g^{\beta_{\mathcal{S}} \Delta y}\ mod\ p\right)$$

Where Δx and Δy represents the difference of integer coordinates which are related to the geographic location of $\mathcal{S}$ and $\mathcal{S}_1$. The obtained geographic location of node $\mathcal{S}$ is available only for the time interval $\Delta\mathcal{S}$.

B. ECDH Key Exchange

During the communication of two neighbouring nodes, a secure session establishment is required which helps to address the different types of attacks such as Man in the Middle attack. Here, node authentication plays important role which helps to avoid the malicious nodes to participate in communication. In order to establish a secured and authenticated communication between two neighboring sensor nodes, we present a hybrid model of ECC (Elliptic Curve Cryptography) and Diffie-Hellman (DH) Key exchange.

(a) Elliptic Curve Cryptography and Diffie-Hellman Key exchange

ECC is known as a promising technique for public-key cryptography which uses elliptic curve structures over a given finite field. This scheme require smaller keys for security when compared with the non-EC cryptography. An elliptic curve $\mathbb{E}$ can be represented in the form of tuples as $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, over a finite filed $\mathbb{F}_p$. This elliptic curve satisfies the equation which is as follows:

$$y^2 = x^3 + ax + b \text{ with } a, b \in \mathbb{F}_p \quad (3)$$

These tuples are called as points which represents the coordinated of x and y. The set of these coordinate points allows to form a cumulative group with the identity elements. Thus, the group operation can be performed using arithmetic operations such as addition, subtraction, multiplication, squaring, and inversion in the given field $\mathbb{F}_p$. Before applying ECC for any cryptographic applications, both nodes must agree to define the elliptic curves which are called as domain parameters which helps to specify the finite field $\mathbb{F}_p$, elliptic curves $\mathbb{E}$, a base point as $P \in E(\mathbb{F}_p)$ to generate the cyclic sub-graphs, and a co-factor as $h = \#\frac{E(\mathbb{F}_p)}{n}$. Similarly, the domain parameters over $\mathbb{F}_p$ are represented in the sextuple form as $\mathbb{D} = (p, a, b, P, n, h)$. According to the Elliptic curve cryptography, the private key is an integer value which is generated from the interval $[1, n-1]$ randomly. The public key is the point $Q = k.P$ on the considered curve.

With the help of these assumptions, we present ECC and DH key exchange approach which is operating in $\mathbb{Z}_p^*$, this approach is called as ECDH. According to the ECDH, a shared secret key is established between two sensor nodes. This process of key exchange is described in the following description using Alice and Bob as two network identities where these identities use same domain parameters as

$\mathbb{D} = (p, a, b, P, n, h)$. According to the ECDH,

- Initially, Alice generates a transitory key pair as (k_A, Q_A). A random number k_A is generated in the time interval as $[1, n-1]$. Later this k_A and prime number are multiplied using scalar multiplication as $Q_A = k_A . P$. later, this generated key Q_A is given to the Bob.
- Similar to the previous stage, bob also generates the transitory key pair as (k_B, Q_B) as $Q_B = k_B . P$ and the generated key $Q_B$is given to the Alice.
- After receiving the public key from the Bob, a shared secret S is generated by Alice by performing a scalar multiplication as $S = k_A . Q_B$
- Similarly, Bob also receives the key from Alice and achieves the shared secret as $S = k_B . Q_A$

At this stage, Alice and Bob contains the same secret S as $k_A . Q_B = k_A . k_B . P$ and $k_B . Q_A = k_B . k_A . P$. due to this process, attacks may get information about public keys of A and B but due to Elliptic Curve Discrete Logarithm Problem, the k_A and k_B cannot be achieved.

This complete process of key exchange, provide the node authentication which helps to avoid the malicious nodes and hence the network information can be secured.

C. ECIS-KEM for Beacon Messages

Geographical routing requires the knowledge of next hop position where data packets are transmitted to the one-hop Neighbour. According to the proposed approach, the location of $\mathcal{S}$ is estimated by $\mathcal{S}_1$ using a continuous beacon message. The neighbouring hop continuously receives the beacon messages from the previous hop and stores the beacon message to facilitate the location information for routing. In proposed approach, we incorporate public key of the node, geographical location and Hashes of neighbouring nodes which are digitally encrypted with the combination of ECC (Elliptic Curve Cryptography) and KEM (Key Encapsulation Method) called as ECIS-KEM.

By making the use of ECC, several approaches have been introduced. Similarly, ECIS is the also developed which is called as "Elliptic Curve Integrated Encryption Scheme" that is based on the key-exchange concept of Diffie-Hellman approach. However, the conventional ECC and ECIS based approaches fail to avoid the chosen cipher text attacks (CCA2) thus a new approach of ECC is developed which uses key encapsulation method to provide the high security when compared with the ECC and ECIS. The ECIS-KEM scheme is implemented in three main stages as key generation, encryption, and decryption.

Let us consider that an elliptic curve E is defined over a finite field F_q and H denotes the group, G represents the prime order of sub-group, μ denotes the order o sub-group and v represents the index of sub-group in H. $\mathcal{E}$ and $\mathcal{D}$ shows encoding and decoding parameters, $\mathcal{E}'$,and $\mathcal{D}'$ represents the partial encoding and decoding parameters, respectively.

A. Key Generation Stage

Here we present key generation steps for ECIS-KEM approach. First of all, select a fully specified group as $\mathcal{G} = (H, G, \boldsymbol{g}, \mu, v, \mathcal{E}, \mathcal{D}, \mathcal{E}', \mathcal{D}')$. Along with this, select two more parameters which are called as $CheckMode$ and $CofactorMode$ and the values of these modes are selected as 0/1. The selection of these modes depends on the value of v.

- If the value of $v = 1$ is then the both modes are 0.
- If $v > 1$ then modes can be set to zero but in this case security degrades by the factor of v
- If $v > 1$ then cofactor mode is set as 1
- One of the mode must be set to 1

Moreover, a group key function also need to be selected which is called as group key derivation function (KDF). Later, a number x is selected randomly as $x \in \{1, .., \mu - 1\}$, with the help of this group element is computed as $h = x\boldsymbol{g}$

B. Data Encryption Phase

Here we present data encryption using key encapsulation ECIS scheme. The main aim of this scheme is to generate a cipher text $\mathbb{C}$ by encrypting the data with the help of a key K where K is the byte string and the length of K is given as $Key_{Len} = ECIS - KEM.OutputKey_{Len}$. the encryption is performed as follows:

- Select a random number r as $r \in \{1, .., \mu - 1\}$
- Compute the generator ad group elements as $\overline{\boldsymbol{g}} = r . \boldsymbol{g}$ and $\overline{\boldsymbol{h}} = r . \boldsymbol{h}$ respectively.
- Generate the cipher text as

$\mathbb{C} = \mathcal{E}(\overline{\boldsymbol{g}})$ or $\mathbb{C} = \mathcal{E}(\overline{\boldsymbol{g}}, format)$ where $format$ specifies the type of encoding used.

Represent the key as $K = KDF(\mathbb{C} || \mathcal{E}'(h), Key_{len})$

C. Data Decryption Phase

Once the data is encrypted, it is transmitted over the secure channel in geographical WSN. The encrypted data is received at the receiver end and decryption is performed. The ECIS-KEM decryption process is as follows:

- Provide the encrypted data $\mathbb{C}$ as the encoded data of the considered group element as $\overline{\boldsymbol{g}} \in \mathcal{H}$. If the encoding of this data is not appropriate then this step fails and process is stopped.
- Check the status of $CheckMode$ and group element, i.e. if the $CheckMode = 1$ and $\overline{\boldsymbol{g}} \in G$ then this step doesn't fail and if the $CheckMode$ and group element conditions are not satisfied, then fails.
- Check the condition of cofactor mode if

$CofactorMode = 1$ then $\hat{g} = v\bar{g}$ and $\hat{g} = v^{-1}x \bmod \mu$ otherwise $\hat{x} = x$ and $\hat{g} = \bar{g}$

- Compute the group element as $\bar{h} = \hat{x}\hat{g}$, if $\bar{h} = 0$ then fail
- Provide the output key as

$K = KDF(\mathbb{C}||\mathcal{E}'(\bar{h}), Key_{Len})$

Based on these assumption, let us consider that a node A is broadcasting the beacon messages periodically which contains several information such as geographical location of the node, randomly selected number, public key K_p, geographic secure Hashes, and Neighbour information list $(\mathbb{I})$. This broadcast message is transmitted to the neighbourhood $\mathcal{N}(A)$ node to the node A, which is represented as $A \to \mathcal{N}(A)$ info $\{\{p, Location(p)\}_p, r_p, K_p, \mathbb{I}, G, M\}_A$ where information $\mathbb{I}$ is represented as $\mathbb{I} \equiv \{\{i, Location(i)\}_i | \ i \in \mathcal{N}(A)\}$, geographical Hash information as $G \equiv \{\langle i, \alpha_i, \beta_i, \gamma_i, \Delta_i, SH(i,A)\rangle | Dist(i,A) < 2R\}$ and $M \equiv \{\langle i, Proof\rangle | \ i \ is \ malicious \ node\}$.

This complete message is encrypted using aforementioned data encryption scheme. According to the proposed approach, the beacon messages are transmitted periodically that helps to validate the routing. In this approach, we present information sharing model between two nodes that helps to reduce the false location attack. Moreover, Geographical hashes are also used to identify the malicious routing behaviour of the node. Based on these assumptions, we present false location attack identification based on the range of the communication node. The beacon messages are stored in the memory storage that contains the location information that is used for detecting the false location attack. The false location attack is identified based on the range R. Each sensor node estimates a location mapping based on the received information from the each Neighbour. In this phase, small location errors are ignored due to localization error but higher errors are considered that neighbouring node is a malicious node. This process of malicious node detection and false location is presented in algorithm 1.

Algorithm 1: Location verification and malicious node detection

Input: Network topology, configuration and one-hop information

Output: Location verification and malicious node detection

Step 1: Malicious Node= [], Neighbour Info= [], and Bad neighborhood =False. (Initial Conditions).

Step 2: While **beacon**

Step 3: $i = Send \ Beacon$ //information message

Step 4: if $Dist(i,A) > R$ // Out of range transmission

$Malicious \ Node = Malicious \ Node + \{i\}$

Step 5: for $r \in Neighbouring \ Nodes \ (i)$// Consider the neighbouring node for one-hop selection

Step 6: if $Dist(i,r) > R$

$Malicious \ Node = Malicious \ Node + \{r\}$ // Out of range transmission

Step 7: if $Dist(i,r) < R \wedge r \notin \mathbb{I}$

$Malicious \ Node = Malicious \ Node + \{r\}$ // Locations are not available in Node information data

$Bad \ Neighbor \ Info \ (r) = true$

$Neighbor \ Info = beacon$

E. Trust Model for Network Security

In this section, we present a trust model to improve the network security based on the one-hop neighbourhood. In order to develop a trust model where direct and indirect trust model are computed, we consider several trust metrics to compute the trust models such as Forwarding, Network Acknowledgement, Packet precision, Authentication, Confidentiality, Reputation responses, Reputation validation and Remaining energy.

(a) Packet Forwarding: according to this trust metric, we identify the node which selectively forward the packets or denies selectively for transmitting the packet. In this process, the node overhears the medium to check whether that the packet was truly forwarded by the selected Neighbour. If this is identified as true then the packet is considered as successful transmission otherwise packet is considered as failure.

(b) Network Acknowledgement: in this metric, we detect the node which has cooperation with other adversaries which are responsible for packet drop and deteriorate the network performance.

(c) Packet precision: in this metric, we consider the packet integrity and measure the quality of packet that no modification in the data has been occurred during the transmission.

(d) Remaining energy: according to this process, along with node availability, and position, the remaining node energy is also considered where if the node has the threshold energy level then it is selected as next-hop.

Based on these four trust values, we compute the direct trust for thee nodes which are already part of the network. Let us consider that node a computes the value for each metric regarding the next hop b, this can be represented as:

$$T_m^{a,b} = \frac{S_m^{a,b}}{F_m^{a,b} + S_m^{a,b}}$$

where $S_m^{a,b}$ denotes the successful cooperation between node a and b, similary, $F_m^{a,b}$ denotes the failure cooperation between node a and b. For these nodes, we use aforementioned four metrics and compute their weighted sum to achieve the direct trust value. This can be expressed as:

$$DT^{a,b} = \sum_{1}^{4} (T_m^{a,b} * W_m)$$

Where W_m denotes the weight of trust metric m, similarly, we compute the indirect trust value for these tow nodes based on their neighbouring responses. The neighbouring nodes are k_1, k_2, k_3 and k_4 ·This indirect trust can be expressed as:

$$IT^{a,b} = \frac{\sum_{l=1}^{4}(DT^{a,k_l} * DT^{,k_l,b})}{\sum_{l=1}^{4} DT^{a,k_l}}$$

Based on these trust values we can improve the network security to by the means of avoiding the malicious node and node reliability. With the help of aforementioned security techniques, the proposed approach is able to handle several attacks which are mentioned below:

- **Black-Hole attack:** according to the proposed approach, the node authentication and trust computation is performed which helps to identify the malicious nodes which are responsible for packet drop during communication.
- With the help of proposed node acknowledgement process, the compromised nodes can be identified due to inappropriate acknowledge message.
- The proposed approach is also able to avoid the modifications or any alteration in the message due to secure key encapsulation method.

Bad-mouthing attack i.e. any node a can provide wrong trust information about the neighbouring node which can lead towards the faulty node selection or packet drop. Proposed approach considers several matrices which makes the collaboration and trust more effective among the neighbouring nodes.

IV. RESULTS AND DISCUSSION

In this section, we present the experimental analysis using proposed (SHAC-GR) Secure Hash, Authentication and Cryptography approach and present a comparative study to show the robust performance of proposed approach. The performance of proposed approach is compared in terms of energy consumption, packet delivery rate, and network throughput for varied simulation time and number of attacker nodes. The complete simulation study is carried out using MATLAB tool running of Windows platform with the configuration as i5 processor, 8GB RAM and 1TB Storage. The considered simulation parameters are presented in below given table 2.

Table.2.Simulatin Parameters

Parameter name	Considered Value
Network Area	1000mx1000m
Number of Sensor Nodes	500
Communication range of node	50 m
Initial energy of node	2J
Energy consumption for transmitting and receiving the packet	0.001J

In this work, we have focused on security and QoS related performance of WSN using secure geographical routing approach and developed a novel approach called as Secure Hash, Authentication and Cryptography based geographical routing for WSN. A discussed in previous sections that geographical routing shows significant improvement in terms of packet delivery and network lifetime because these routing do not require complete information about the network path. In contrast to this, we present a multi-stage security model that provides security to geographical locations by generating Hashes, node authentication, key encapsulation based cryptography and trust computation. However, more security computation s require more time and consumes more energy but also improves the network reliability and performance i.e. network lifetime, throughput etc. To address the, security and performance related issues, here we present a control parameter window $(\mathcal{F})$ that is defined in the range of [0, 1]. This range depends on the stages considered for security. In other words, we can select or discard the applied security according to the requirement. Let us consider a scenario where our aim is to provide the more security, in that case control parameter window $(\mathcal{F})$ is set to 1 which considers all security aspects such as location security, node authentication, cryptography and trust model. Similarly, if less security is considered, for example if only location security is needed then the control parameter window $(\mathcal{F})$ is set to 0.25 as $\mathcal{F} = 0.25$, if authentication and location privacy is needed the $\mathcal{F} = 0.5$, if location, authentication and cryptography are required then $\mathcal{F} = 0.75$. Based on this variation of control parameter window, we evaluate and compare the performance of proposed SHAC-GR. Based on these parameters, we compute the energy consumption performance for varied security parameters. Figure 2 shows a comparative performance in terms of energy consumption. This performance is measured for varied number of sensor nodes

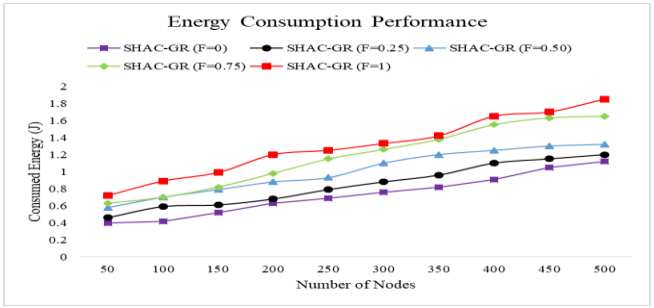

Fig.2. Energy consumption performance

With the help of this study, we can show that the energy consumption increases if required number of security parameters are increasing. In this study, the average energy consumption is obtained as 0.732, 0.842, 1.005, 1.175 and 1.3 J for $\mathcal{F}$=0,0.25,0.5,0.75 and 1, respectively.

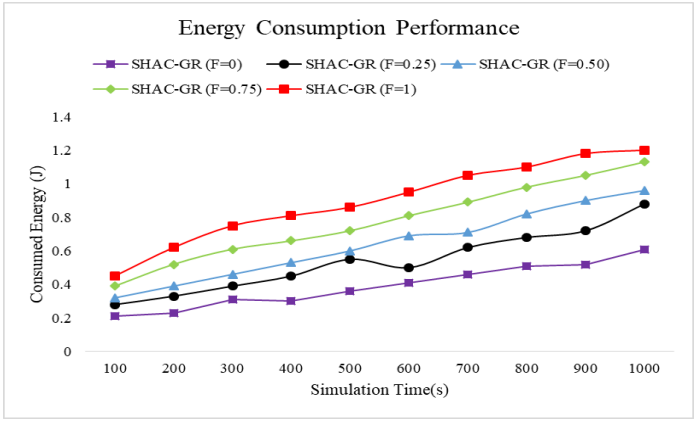

Fig.3. Energy consumption based on simulation time

In figure 3, we present the energy consumption performance for varied simulation time from 100 sec to 1000 sec.

Similar to the previous experiment, in this study also, energy consumption performance is measured. More security requires more computation resulting in the increased energy consumption. We obtain the average energy consumption as 0.39, 0.54, 0.63, 0.77 and 0.89J for $\mathcal{F}$=0,0.25,0.5,0.75 and 1, respectively.

Figure 4 shows a comparative performance in terms of packet delivery rate based on the varied number of malicious node. In order to evaluate this performance analysis, we have considered varied number of malicious nodes. For experiment $\mathcal{F}$=0, we achieve the poor performance when compared with the other steps because no security parameters are implemented in this phase and hence the malicious nodes causes packet drop during data transmission to the next-hop.

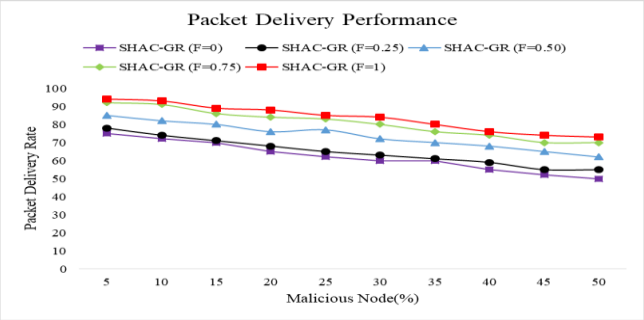

Fig.4. Packet delivery performance for varied number of malicious node

The average packet delivery rate is obtained as 62.1%, 64.9%, 73.7%, 80.6% and 83.6% using control parameter window as $\mathcal{F}$=0,0.25,0.5,0.75 and 1, respectively. Similarly, we compute the network throughput performance for varied malicious nodes because the malicious nodes causes packet drop due to different types of attack. The impact of malicious nodes can be identified based on the system throughput. Figure 4 shows a comparative performance for different number of malicious nodes and control parameter window.

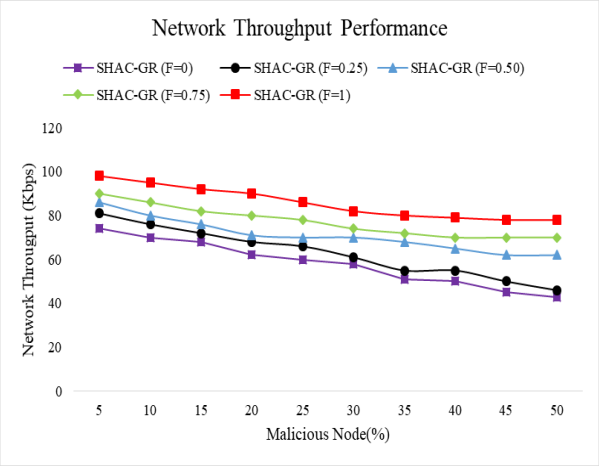

Fig.5. Network Throughput performance

According to figure 5, the network throughput performance is obtained as 58.1%, 63%, 71%, 77.2% and 85.8% using control parameter window as $\mathcal{F}$=0,0.25,0.5,0.75 and 1, respectively.

V. CONCLUSION

In this work, we have focused on the geographical routing in wireless sensor networks. Generally, WSNs suffer from the energy consumption related issues, which is a challenging task for research community, similarly, security, and privacy is a crucial task in this field of geographical WSN. These two parameters have significant impact on the network performance. Limited work has been presented which can control both the parameters simultaneously. Motivated by this issue, we present a combined approach to improve the network security and energy consumption performance. The complete proposed approach follows geographical routing protocol where complete network information is not required and end-to end path is not computed initially whereas next hop is computed hence it consumes comparatively less energy. On other hand, these routing protocols are vulnerable to security threats hence to address the security issues we present Hash based location privacy model, ECDH key management scheme, encapsulation based ECIS-KEM approach for data encryption and finally a trust model is developed to make a decision for next hop selection. This approach reduces malicious node count hence packet drop reduces and delivery rate increases. However, if energy consumption minimization is main objective, then number of security operations can be reduced using a control parameters. A comparative experimental study is carried out which shows that proposed approach achieves better performance for varied control parameters in terms of energy and packet delivery.

REFERENCES

1. Banimelhem, O., & Khasawneh, S. (2012). GMCAR: Grid-based multipath with congestion avoidance routing protocol in wireless sensor networks. Ad Hoc Networks, 10(7), 1346-1361.
2. Rawat, P., Singh, K. D., Chaouchi, H., & Bonnin, J. M. (2014). Wireless sensor networks: a survey on recent developments and potential synergies. The Journal of supercomputing, 68(1), 1-48.
3. García-Hernando, A. B., Martínez-Ortega, J. F., López-Navarro, J. M., Prayati, A., & Redondo-López, L. (2008). WSN application scenarios. In Problem Solving for Wireless Sensor Networks (pp. 1-33). Springer, London.
4. Dong, Y., Wang, J., Shim, B., & Kim, D. I. (2016). DEARER: A distance-and-energy-aware routing with energy reservation for energy harvesting wireless sensor networks. IEEE Journal on Selected Areas in Communications, 34(12), 3798-3813.
5. Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K., & Khan, A. W. (2015). TERP: A trust and energy aware routing protocol for wireless sensor network. IEEE Sensors Journal, 15(12), 6962-6972.
6. Gong, P., Chen, T. M., & Xu, Q. (2015). ETARP: An energy efficient trust-aware routing protocol for wireless sensor networks. Journal of Sensors, 2015.
7. Tanwar, S., Kumar, N., & Rodrigues, J. J. P. C. (2015). A systematic review on heterogeneous routing protocols for wireless sensor networks. Journal of Network and Computer Applications, 53, 39–56.
8. Naik, S., & Shekokar, N. (2015). Conservation of energy in wireless sensor network by preventing denial of sleep attack. Procedia Computer Science, 45, 370-379.
9. Vasserman, E. Y., & Hopper, N. (2013). Vampire attacks: draining life from wireless ad hoc sensor networks. IEEE transactions on mobile computing, 12(2), 318-332.
10. Elhoseny, M., Elminir, H., Riad, A., & Yuan, X. (2016). A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption. Journal of King Saud University-Computer and Information Sciences, 28(3), 262-275.
11. Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). ActiveTrust: secure and trustable routing in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 11(9), 2013-2027.

12. Kaur, J., Gill, S. S., & Dhaliwal, B. S. "Secure trust based key management routing framework for wireless sensor networks". Journal of Engineering, 2016.
13. Lyu, C., Gu, D., Zhang, X., Sun, S., Zhang, Y., & Pande, A. (2015). SGOR: Secure and scalable geographic opportunistic routing with received signal strength in WSNs. Computer Communications, 59, 37-51.
14. Tang, D., Li, T., Ren, J., & Wu, J. (2015). Cost-aware secure routing (CASER) protocol design for wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, 26(4), 960-973.
15. Shi, E., & Perrig, A. (2004). Designing secure sensor networks. IEEE Wireless Communications, 11(6), 38-43.
16. Jiang, P., Wen, Y., Wang, J., Shen, X., & Xue, A. (2006, June). A study of routing protocols in wireless sensor networks. In Intelligent Control and Automation, 2006. WCICA 2006. The Sixth World Congress on (Vol. 1, pp. 266-270). IEEE.
17. Sabor, N., Sasaki, S., Abo-Zahhad, M., & Ahmed, S. M. (2017). A comprehensive survey on hierarchical-based routing protocols for mobile wireless sensor networks: review, taxonomy, and future directions. Wireless Communications and Mobile Computing, 2017.
18. Kumar, A., Shwe, H. Y., Wong, K. J., & Chong, P. H. (2017). Location-Based Routing Protocols for Wireless Sensor Networks: A Survey. Wireless Sensor Network, 9(01), 25.
19. Zabin, F., Misra, S., Woungang, I., Rashvand, H. F., Ma, N. W., & Ali, M. A. (2008). REEP: data-centric, energy-efficient and reliable routing protocol for wireless sensor networks. IET communications, 2(8), 995-1008.
20. Rehena, Z., Roy, S., & Mukherjee, N. (2011, January). A modified SPIN for wireless sensor networks. In Communication Systems and Networks (COMSNETS), 2011 Third International Conference on (pp. 1-4). IEEE.
21. Mann, P. S., & Singh, S. (2017). Energy-efficient hierarchical routing for wireless sensor networks: a swarm intelligence approach. Wireless Personal Communications, 92(2), 785-805.
22. Zhang G, Zhang Y, Chen Z. Using trust to secure geographic and energy aware routing against multiple attacks. PloS one. 2013 Oct 21; 8(10):e77488.
23. Wang, J., Zhang, Y., Wang, J., Ma, Y., & Chen, M. (2015). PWDGR: pair-wise directional geographical routing based on wireless sensor network. IEEE internet of things journal, 2(1), 14-22.
24. Vamsi, P. R., & Kant, K. (2016). Trust and location-aware routing protocol for wireless sensor networks. IETE Journal of Research, 62(5), 634-644.
25. Muthusenthil, B., & Murugavalli, S. (2017). Privacy preservation and protection for cluster based geographic routing protocol in MANET. Wireless Networks, 23(1), 79-87.
26. Punitha, A., & Manickam, J. M. L. (2017). Privacy preservation and authentication on secure geographical routing in VANET. Journal of Experimental & Theoretical Artificial Intelligence, 29(3), 617-628.
27. Thevar, G. K. C., & Rohini, G. (2017). Energy efficient geographical key management scheme for authentication in mobile wireless sensor networks. Wireless Networks, 23(5), 1479-1489.
28. Zaimi, I., Boushaba, A., Houssaini, Z. S., & Oumsis, M. (2018). A fuzzy geographical routing approach to support real-time multimedia transmission for vehicular ad hoc networks. Wireless Networks, 1-23.
29. D. R. Manjunath and S. N. Thimmaraju.(2019). A Path Blind Approach to Secure Geographical Routing in Energy Aware Wireless Sensor Networks. J. Comput. Theor. Nanosci. 16(6), 2555–2566.
30. Wagner, D., & Wattenhofer, R. (2007). Algorithms for sensor and ad hoc networks: advanced lectures. Springer-Verlag.
31. Adnan, A. I., Hanapi, Z. M., Othman, M., & Zukarnain, Z. A. (2017). A Secure Region-Based Geographic Routing Protocol (SRBGR) for Wireless Sensor Networks. PloS one, 12(1), e0170273.

AUTHORS PROFILE

Manjunath D R is currently working as assistant Professor in Dept. of CSE , Dayananda Sagar Academy of Technology and Management, Bangalore, received B.E and M.Tech in Computer Science and Engineering from Visvesvaraya Technological University, Belagavi, Karnataka, India, 2007 and 2013, and he is currently pursuing the PhD in Computer Science and Engineering from Visvesvaraya Technological University.

Dr. Thimmaraju S N is a Professor in Dept. of Masters of Computer Applications, Visvesvaraya Technological University, and Centre for Post Graduate Studies, Mysore, India. His research interests lie in the areas of computer networking, graph theory and big data