A Hybrid Encryption Technique for Secure-GLOR: The Adaptive Secure Routing Protocol for Dynamic Wireless Mesh Networks[1]

Ashish Nanda[1], Priyadarsi Nanda[1], Xiangjian He[1], Aruna Jamdagni[2] and Deepak Puthal[1]
[1]School of Computing and Communications, Faculty of Engineering and IT
University of Technology, Sydney, Australia
Ashish.Nanda@student.uts.edu.au,
{Priyadarsi.Nanda, Xiangjian.He, Deepak.Puthal}@uts.edu.au
[2]Western Sydney University, Sydney, Australia
A.Jamdagni@westernsydney.edu.au

Abstract
As we progress in into a digital era where most aspects of our life depend upon a network of computers, it is essential to focus on digital security. Each component of a network, be it a physical network, virtual network or social network requires security when transmitting data. Hence the dynamic wireless mesh network must also deploy high levels of security as found in current legacy networks. This paper presents a secure Geo-Location Oriented Routing (Secure-GLOR) protocol for wireless mesh networks, which incorporates a hybrid encryption scheme for its multilevel security framework. The hybrid encryption technique improves the network's overall performance compared to the basic encryption by using a combination of symmetric key as well as asymmetric key encryption. Using the combination of the two encryption schemes, the performance of the network can be improved by reducing the transmitted data size, reduced computational overhead and faster encryption-decryption cycles. In this paper discussed multiple encryption schemes for both symmetric and asymmetric encryption, compare their performance in various experimental scenarios. Proposed security scheme achieves better performance based on the results obtained with most viable options for our network model.

Keywords
Geo-Location Oriented Routing (GLOR), Smart Device Network, Secure-GLOR, Secure Mesh Networks.

[1] The preliminary version of this paper is presented in the IEEE TrustCom 2017 [21].

1. Introduction

With the advancements in technology, the digital world impact various aspects of our lives and has become an essential part of our daily commute. The communication network is one of the most important part keeping us connected to the digital world. We rely on the communication network to access the internet, control traffic, make payments and even carry our sensitive data, hence it is essential that it maintains high levels of security to ensure the integrity of the network.

The continuously rising need for security is now expanding to every type of network, be it social or physical. This need for security has also come to wireless mesh networks that have been in development over the past years. The mesh networks are known for their ability to form self-sustained and easily configurable network by connecting large number of devices together, however guaranteeing security in such network is one of the major issues for future application specific deployments. Unlike the legacy networks, the mesh networks depend on its devices to relay the data by sending it through a chain of devices, which means that the data is accessed by more than just the device it was destined for. Hence the need for securely delivery of data is very critical to the future of such network model [6].

In addition, the dynamic wireless mesh networks require a custom-tailored security framework as the current/legacy security solutions doesn't fit well and limit its capabilities. This is because the present security solutions for mesh network requires a central entity dependant network which limits the size and dynamic-ness when applied to the wireless mesh network. In this document, we present the Secure-GLOR model based upon the GLOR protocol. The Secure-GLOR model is specifically designed to embrace the dynamic properties of a wireless mesh network while providing high level of security.

A Summary of the contributions made by this paper are as follows:

1. An introduction to the Secure-GLOR model, the GLOR protocol and its components.
2. A brief overview of a scenario based authentication scheme for Secure-GLOR
3. A hybrid encryption technique for the Secure-GLOR model using a combination of well-known symmetric and asymmetric encryption techniques.
4. Performance analysis for various symmetric and asymmetric encryption techniques.
5. Performance analysis of basic and hybrid encryption techniques for the Secure-GLOR network model.

This paper introduces the hybrid encryption scheme for the secure version of the GLOR protocol, as proposed in the previous papers [8,21]. Section 2 of this paper begins with a discussion about related approaches/models and how they implement security. Section 3 briefly presents the GLOR protocol and its various features and how it stands apart from other protocols. The security model and its various aspects implemented by the GLOR protocol is then explained in Section 4 followed by a theoretical analysis of the model in Section 5. Section 6 presents the performance of the network model under different scenarios with various configurations and discusses the results obtained. Finally, Section 7 concludes with the final thoughts on the next step of Secure-GLOR protocol.

2. Related Works

Amongst the models/approaches that propose a totally dynamic self-sustained wireless mesh networks, very few take in account the security of data being transmitted.

The Smart Phone Ad hoc Networks (SPAN) project [1] was the earliest practical implementation showing an off-grid network; however, the project had no current security implementation. Though it discusses the use of public-private key pair for encrypted communication between devices, the key exchange process was manual and a major risk.

Several Project [3] and FireChat [4] are other similar implementations which use Wi-Fi/Bluetooth to create a self-sustained network. However, the methodology lacks security as each message is sent to every device on the network without any encryption, like a chat room.

The BRIAR Project [5] has been designed to provide secure and resilient peer to peer communications with no centralized servers and minimal reliance on external infrastructure. The approach implements high levels of security using end-to-end encryption to prevent keyword filtering. However, to implement high levels of security, the devices don't communicate directly unless their owners have common contacts. In other words, device ‘A’ can communicate with a device ‘C’ through another device ‘B’ only if the device ‘A’ and device ‘C’ exist as contacts on device ‘B’. This makes it difficult for the network to expand or improve functionality.

There are several security threats in wireless communication networks, the layer wise classification of the security threats and solutions are given in [17]. In [13,14], it is already proven that symmetric key solutions are thousand times faster than asymmetric key solutions. Symmetric key cryptography is always suitable for the low power devices, where shared key needs to be updated after certain period [15]. Current research trends create hybrid architecture by combining communication and computing technologies such as fog or cloud computing. In [16,18] authors have given the novel security solutions for these hybrid architectures. Cheikhrouhou et al. [19] have proposed an authentication architecture for wireless mesh networks, which also designed to maintain data confidentiality. By following above specified security solutions, we have applied both symmetric key cryptography and asymmetric key cryptography for our proposed GLOR protocol.

3. Geo-Location Oriented Routing (GLOR)

Geo Location Oriented Routing (GLOR) [7,20] is a hybrid routing protocol designed to support large, dense & dynamic networks without compromising the reliability and security of the network and the devices in it. The protocol is specifically designed for the high-performance devices such as smartphones, tablets, laptops, etc. which possess a high processing power and a means to communicate with other devices. Following is an outline of the major features of the GLOR protocol.

- **Reverse Network Model:** The devices (referred to as nodes) are responsible for maintaining the network. Tasks include node address calculation, node registration, node monitoring, packet routing, address allocation etc. are monitored by the nodes.
- **New Addressing Scheme:** The smart approach uses geo-location of a device as its IP address (described in Section 3.1). The geo-location is obtained using GPS or is calculated by nearby

nodes. This provides us to determine the instantaneous position of each node, like dots on a fixed canvas.

- **Smart Packets:** The new data packet has been modified to take advantage of the new addressing scheme. The packets are supplied with the destination node's address and can dynamically decide its own path (described in Section 3.2).
- **Security Model:** The network model also implements authentication and encryption to improve the security of the network. The Model is further explained in Section 4.

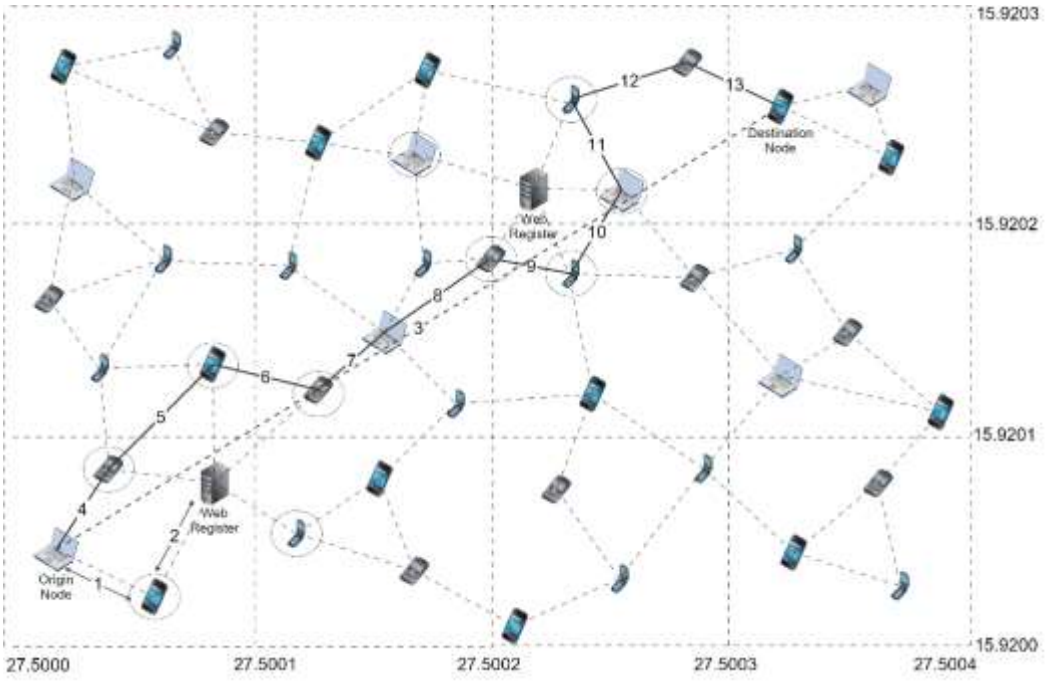

Fig. 1. Different Components of Routing Process

As shown in Fig. 1, the node is an electronic device (e.g. Smart-Phone, Laptop, and Tablet) that implements Geo-Location Oriented Routing (GLOR). It can be classified and a normal node and a web node based on their connectivity. A normal node has the capability to connect to other devices wirelessly while implements GLOR protocol, the web node a normal node with the additional capability to connect directly to the Web Register. A node X is said to be the neighbor node of Y if there exists a link between the node X and node Y.

The nodes can be identified using two factors, the node address and the unique ID. The node address is the Geo-Location of the Node, i.e. its latitude and longitude measured up to 4 decimal places and the node's unique ID is a onetime generated Unique Identification number assigned to the Node alongside its MAC address during its first registration on the network. The web register is a cloud-based database dedicated for storing vital information about nodes, including their MAC address, unique ID, address, and current state. The Sector for a Node can be defined as a group of its neighboring nodes. This helps improve the accuracy as each node in a sector knows other nodes in that sector.

3.1 Node Addressing

The GLOR protocol uses Geo Location in place of the IP address for the nodes. This is achieved by using the IPv6 addressing format that uses 32 hexadecimal bits and dividing it into eight groups of 4 hexadecimal bits each.

The first 2 group store the Latitude, with the first bit representing '+' (as 0) or '-' (as 1), similarly the next 2 group store the Longitude as shown in Fig. 2. Each bit represents 10^n meters, where n is the position of the bit (starting from right to left).

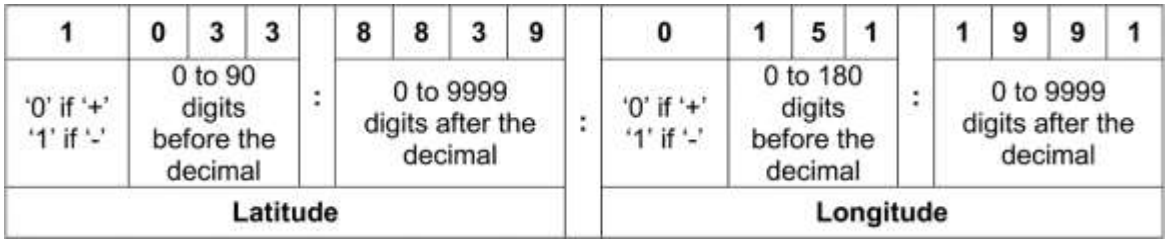

Fig. 2. Addressing scheme (Part 1)

The next 4 groups store the cluster number and the sector number. Each sector represents 100 square meters of land and is defined using the Latitude-Longitude system. The cluster is a combination of predefined sectors. Fig. 3 explains the Sector-Cluster structure used.

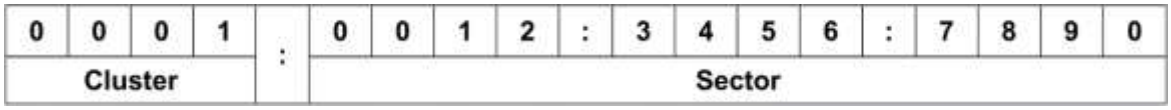

Fig. 3. Addressing scheme (Part 2)

The Sectors and Clusters are calculated automatically based on the current Latitude and Longitude of the node. This is based on International Standard representation of geographic point location by coordinates.

3.2 Smart Packets

As discussed in the beginning of Section 3, the GLOR protocol uses a modified version of the basic data packet as shown in Fig. 4. It's designed to be simple yet contain enough information that it can calculate its own route once it has left the origin node. The packet selects the next hop using the geo-location of the source node and the destination node. Using these two location details as two points on a graph a straight line is plotted and then the neighbor node closest to the line and farthest to the Source Node is selected and the packet is transmitted to it. This process repeats itself until the packet has reached its destination.

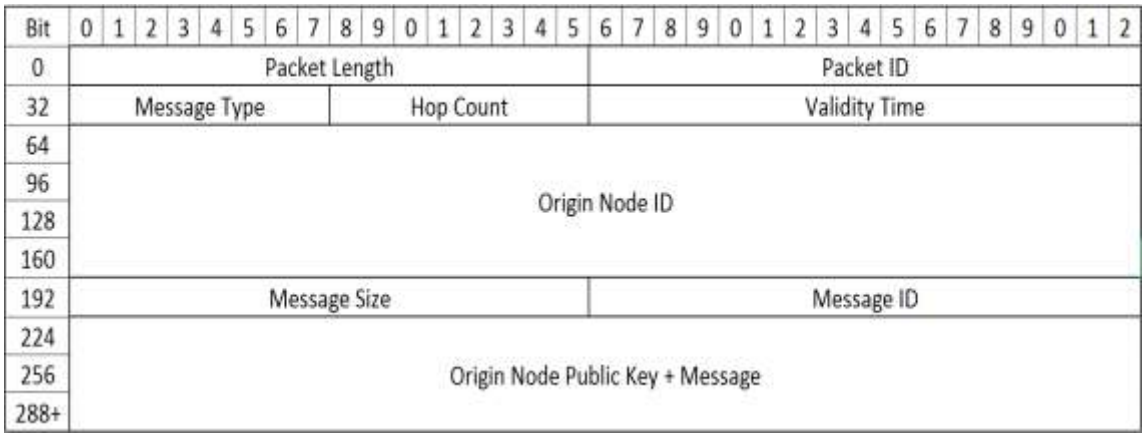

Fig. 4. Packet Format (Omitting TCP/IP Headers)

The simple design and minimized header size helps the packets carry more data and reduce overhead. Various components of the packet are described below.

- Packet Length - It is the length of the packet (in bytes).
- Packet ID - The Packet ID or PID is an identifier and must be incremented by one each time a new GLOR packet is transmitted
- Message Type - It indicates the type of the message that is being transmitted.
- Hop Count - It is the number of hops a message has attained. It is incremented every time the packet is retransmitted.
- Validity Time - It is the maximum time during which the information of the packet is considered valid. If a node receives a packet with Validity Time = 0, the packet is discarded.
- Origin Node ID - This is the ID of the node that originally generated the packet. It is not to be confused with the Source Node ID in the IP header as the Source ID is updated each time to the address of the intermediate node whereas the Origin Node ID remains constant.
- Message Size - It is the total size in bytes measured from the beginning of "Message Type" till the end of the message.
- Message ID - A unique ID is provided to each message by the Origin Node. It is incremented by one for each message. As a message can be divided into multiple packets, Message ID helps in identifying the separately received packets and group them accordingly.
- Origin Node Public Key – It is the public key of the origin node that is to be used by the destination node for encrypting any data it wishes to send back.
- Message – It is the actual data being sent to the destination node.

3.3 Web Register

As referred to in the beginning of Section 3, the web register is a cloud based dedicated database used to store device information. It can be accessed by any authenticated node that has access to the internet, or through a neighbor node which possesses internet access. The web register acts as the yellow pages of the network and improves the performance and accuracy of the network.

Web register, being a key element of the network, is not a central or control node. The network can function without its presence by following a Sector-Broadcast Progression. According to this method, the origin node sends out packets aimed in the direction of its four neighbouring sectors. As each node keeps a record of all the devices in their sector, it can check if the destination node exists in the sector. If yes then the packet is relayed to it, if not then the packet is forwarded to the neighbouring sector. In comparison to simple broadcast method, the sector-broadcast helps lower the load on the network.

3.4 Packet Creation

Before the origin node can send a packet, it requests the web register for details about the destination node by providing the destination node's unique ID. The web register checks for the details associated with the unique ID and responds accordingly.

Once the web register locates the details, it also checks if the destination node is still connected to the network. When the verification is complete, the details are then sent to the origin node and are used to create the smart packet. Please refer to [7], for more details about the packet processing and forwarding.

4. Security Model

The GLOR protocol implements a very basic but effective security model [8]. It is implemented through different network levels, and each level focuses on an important aspect of routing. The two aspects are authentication and encryption and are explained below in detail.

Table 1: List of Components

Term	Component	Description
Node	Network Device	A device with established connection to the network and is authorized to authenticate other devices.
Device	New Device	A device which wishes to join the network.
WR	Web Register	A database that stores network device information such as Unique ID, MAC, Address, Public Key, etc.
UID	Unique ID	A unique identifier generated and provided to each node by the Web Register. It is linked with each device's MAC.
ADDR	Geo-Location Address	Physical position (two dimensional) of the device determined through its latitude and longitude coordinates

K_{PU}	Public Key	Asymmetric encryption key pair used for authentication and End-to-End encryption. Each device gets its own key pair.
K_{PI}	Private Key	
K_{SE}	Session Key	Symmetric encryption key provided to each device at registration.

4.1 Encryption

The second most essential part of a network's security depends upon how best it can secure the data while its being sent across the network. The Secure-GLOR model was originally designed to use asymmetric encryption algorithm to avoid refreshing encryption keys frequently. However, the model has been updated to use a hybrid encryption technique to overcome the delays caused when transferring bigger chunks of data.

4.1.1 Original Encryption Technique

In the original paper [21] we used RSA to encrypt the message part of the smart packet. It begins during the packet formation process after the origin node requests for the details of the destination node. Each node generates a new public-private key pair during its first registration during which it also sends a copy of the public key to the web register. This comes in handy when a node wishes to send some data.

Algorithm 1. Key Management

$K_{PR}(i)$ – Private Key of node *i*

$K_{PU}(i)$ – Public Key of node *i*

WR - Web Register; SN - Source Node; DN - Destination Node

1. At initial node registration

   ∀ node *i* generates its key pair i.e. $K_{PR}(i)$ and $K_{PU}(i)$

2. Nodes share own public key with web register (WR)

   $K_{PU}(i) \rightarrow$ WR

3. During data transmission

   SN (request) → WR (DN location)

   If WR authenticate SN and found DN in the register

   WR → SN: ($K_{PU}(DN) \parallel Loc\ (DN)$)

   Then SN uses $K_{PU}(DN)$ for data encryption.

As explained in Section 3.4, once the node receives information about the destination node, it also receives the public key of the destination node. This is used to encrypt the message part of the packet such that only the destination node can decrypt it using its own private key. In addition to encrypting the message, the node also provides its own public key that the destination node can use to encrypt any response it wishes to send. The complete procedure for key management in Secure-GLOR is shown in Algorithm 1.

4.1.2 Hybrid Encryption Technique

The asymmetric encryption performed similar to the symmetric encryption with small data set. However, during the implementation and testing phase it was discovered that symmetric encryption algorithms performed considerably better compared to the asymmetric encryption algorithms when a larger data size was used. Due to the fact that asymmetric algorithms can only encrypt data set of size smaller than the key, it takes multiple iterations for larger data sets as they are broken down into smaller chunks and then individually encrypted. This is however not the case with symmetric algorithms as they encrypt in a single iteration.

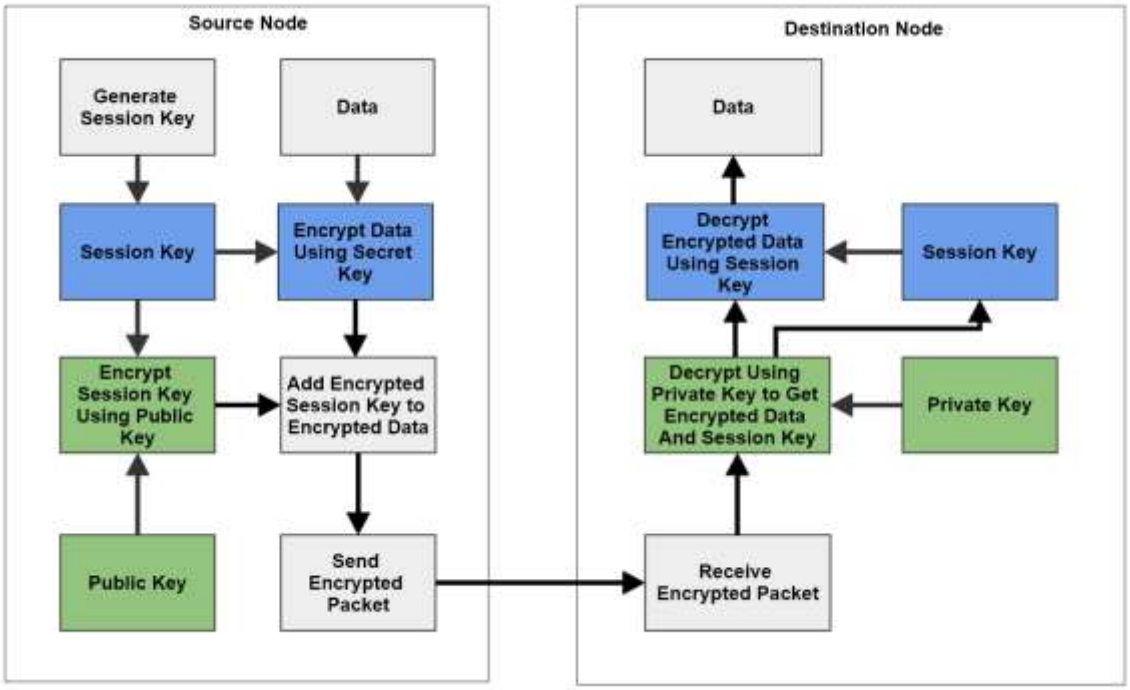

Fig. 5. Hybrid Encryption

In order to provide better and faster encryption/decryption cycles for the Secure-GLOR model, we use the hybrid encryption scheme. According to the hybrid encryption scheme, a symmetric encryption technique is used to encrypt the data while the asymmetric encryption algorithm is used to encrypt the key used by symmetric encryption. The essence of hybrid encryption is the use of session key (symmetric encryption) which are randomly generated and exchanged between the source node and destination node. To ensure the session key is not stolen or tampered with, the asymmetric encryption is used to encrypt the session key using the public key of the destination node ensuring that only the destination node can access the session key and using it decrypt the data as shown in Fig. 5.

Algorithm 2. Session Key Management

$K_{PR}(i)$ – private key of node *i*

$K_{PU}(i)$ – public key of node *i*

$K_{SE}(i)$ – session key

WR - web register; SN - sender node; DN - destination node

1. At initial node registration

   ∀ node *i* generates its key pair i.e. $K_{PR}(i)$ and $K_{PU}(i)$

2. Nodes share own public key with web register (WR)

   $K_{PU}(i) \rightarrow$ WR

3. Before Data transmission

   SN (request) → WR (DN location)

   If WR authenticate SN and found DN in the register

   WR → SN: ($K_{PU}(DN) \parallel Loc\ (DN)$)

4. Generate Session Key

   SN(Random) → K_{SE}

   SN uses K_{SE} for data encryption.

5. Session Key Encryption

   SN uses $K_{PU}(K_{SE})$ for session key encryption.

   Encrypted (data & K_{SE}) are concatenated and sent

4.2 Authentication

The Secure-GLOR implements a scenario based hybrid authentication mechanism as explained in [22]. Authentication is an important initial security phase responsible of granting network access to a device based. Unlike various other schemes where a device connects to the network and is then authenticated, Secure-GLOR does not allow network access and hence keeps the device in a sandbox scenario until the authentication process is completed and a decision has been made.

The type of access being granted depends on various aspects which are collected in the form of device information or calculated through a mathematical challenge. The scenario based authentication also considers the various conditions a device might face during the authentication process and accordingly decides upon the authentication scheme to be used and the type of network access to be granted.

The authentication process begins when a device requests connection to the network. The process is initiated by one of the nodes (a device which is a part of the network) when is receives a network access request. The node must then collect the device information including the unique ID, MAC address, Location, etc. Once the details are collected, the node must decide upon an authentication scenario as shown in Fig. 6.

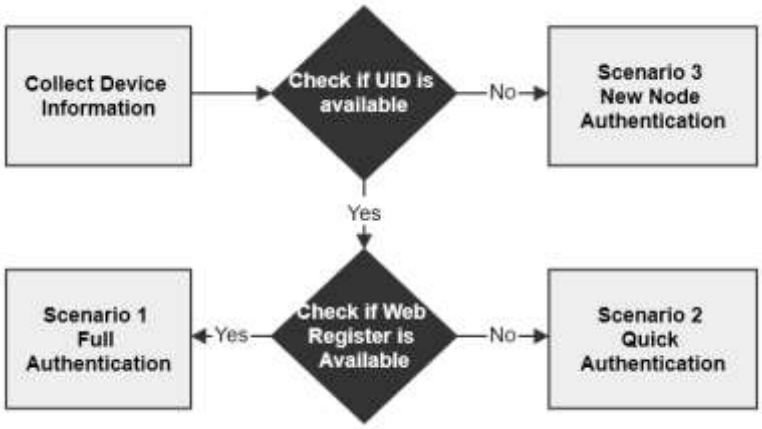

Fig. 6. Authentication Scenario Selection.

The three authentication scenarios are as follows:

Full Authentication: In this scenario, a device is reconnecting to the network and is authenticated by a Node which, has a direct or indirect link to the web register. On successful authentication, the network device will grant the new device network access along with the right to authenticate other devices.

Quick Authentication: In this scenario, the device is reconnecting to the network and is authenticated by a network device which does not possess a direct or indirect link to the web register at the moment. In this scenario, the network device itself carries out the authentication. On successful authentication, the new device is granted network access but not the right to authenticate new devices until the network device has verified the new device's information with the web register.

New Node Authentication: In this scenario, an unregistered device (which has never connected to the network) wants to join the network. For this scenario, it is vital that the network device maintains a direct or indirect access to the web register. This is required as all the device information collected must be recorded at the web register for pre-registration authentication and the registration process as depicted in Fig. 7.

The authentication scheme incorporates challenge-response technique and uses a mathematical equation along with the encryption keys to verify the device. All the encryption keys that are used during the authentication process are stored in a TPM (Trusted Platform Module) which prevents any unauthorized access to the sensitive information if a device on the networks is internally compromised.

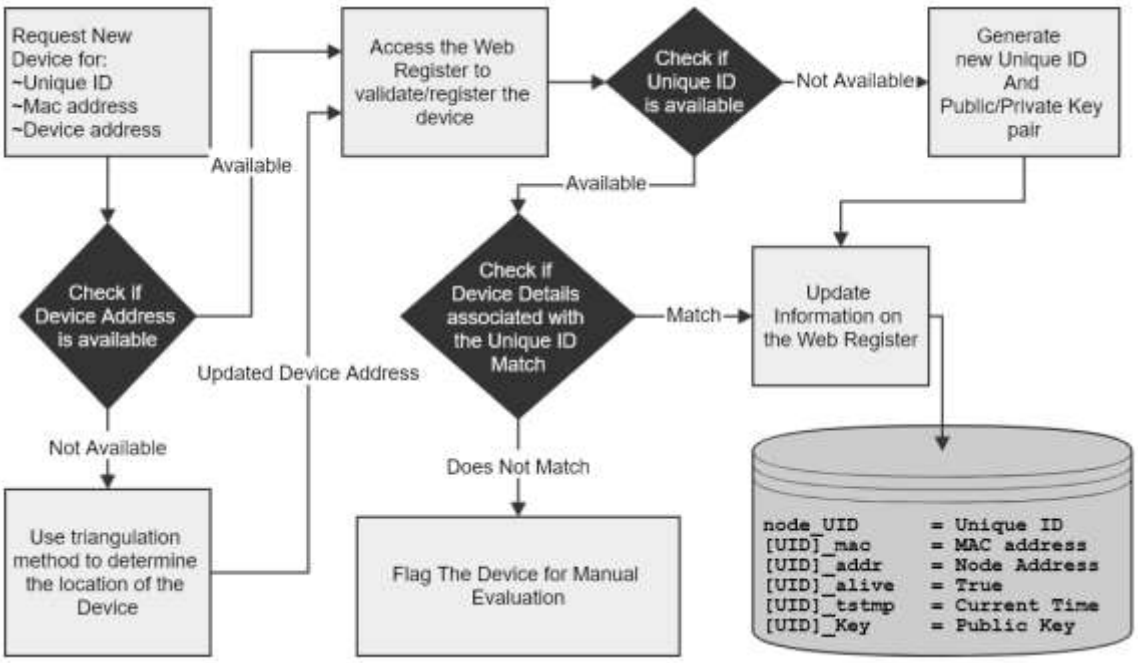

Fig. 7. Node Registration Process.

5. Theoretical analysis

This section provides a theoretical analysis of our proposed Secure-GLOR model to demonstrate its response to potential security threats and how Secure-GLOR is protected against them. We use hybrid encryption where asymmetric key cryptography is used to protect the session key and symmetric key cryptography is used to protect data in the dynamic mesh network. The proposed security method performs efficiently without degrading network performance.

We have made the following practical and realistic assumption in our method:

Assumption 1. In our method, the data that is encrypted by a symmetric-key method cannot be decrypted by any other, unless they have the session key.

Assumption 2. In our method, the session key that is encrypted by an asymmetric-key method cannot be decrypted by any other, unless they have the private key.

5.1 Security proofs

Definition 1 (attack on integrity): A malicious attacker M*i* can attack the integrity if it is an adversary capable of monitoring the data packets regularly and trying to access and modify them before they reach their destination.

Definition 2 (attack on confidentiality): A malicious attacker M*c* is an unauthorized party which has ability to access or view the unauthorized data packets before they reach the destination node.

Theorem 1: Proposed Secure-GLOR maintains end-to-end security in mesh network with dynamic nodes.

Proof: We used an asymmetric key cryptographic method to maintain end-to-end security over our GLOR protocol in dynamic wireless mess network. As our network model comprises of high performance devices (i.e. smartphones, laptop, etc.), hence we prefer to reduce number of keys in use and hence, reduce the network overhead.

In symmetric key cryptography with n number of nodes, the number of pairwise keys calculated for secure communication is as below:

If a new node i is added to the network, it needs to share a new key with other nodes.

Then for n users, we have $1 + 2 + \cdots + (n-1) = \frac{n(n-1)}{2}$ keys.
$\Rightarrow$ there will be $O(n^2)$ keys.

In a similar way, for asymmetric key cryptography with n number of nodes, the number of pairwise keys calculated for secure communication are as below:

If a new node i is added to the network, it needs only a public key and a private key to share a new key with other nodes.

Then for n users, we have $2n$ keys.
$\Rightarrow$ there will be $O(n)$ keys.

While comparing with other existing symmetric key algorithms, individual nodes may need separate pair, so in result we have $4n$ keys i.e. $O(n)$ keys.

Another advantage with asymmetric key over symmetric key algorithm is that it does not require changing or updating the key after a certain interval of time, which leads to reduced network communication overhead and loss of secret keys. Our security method uses public key (K_{PU}) to encrypt and private key (K_{PR}) to decrypt the session key (K_{SE}), and each node only shares its public key with web register. Hence, an intruder might reach the web register to obtain the public key but it's impossible to get the private key as the node never shares it with anyone.

Finally, only recipient node can decrypt the packet using own private key (K_{PR}) to get the session key and using it decrypt the data. Therefore, we can conclude that Secure-GLOR maintains end-to-end security.

Theorem 2: Secure-GLOR is secure against attack on integrity and confidentiality

Proof: Following *Algorithm 1*, it is clear that the intruder cannot get the destination node's private key to decrypt the data packet.

Following *Definition 1*, we know that an attacker M_i has full access to the network to read data flow, but M_i cannot get private key information of destination node such as K_{PR}. Intruder can get the public key K_{PU} but it's useless as there is no such method to obtain/derive the private key using public key. In the same way following *Definition 2*, M_c can gain access to the public key K_{PU} but no other information.

Finally, M_i and M_c can neither read nor modify the data packets, it can only be accessed by the destination node. Hence, Secure-GLOR is secure against an attack on integrity and confidentiality.

5.2 Forward secrecy

By following a standard asymmetric key cryptography procedures, destination node's public key is used to encrypt the session key which in turn encrypts the data packets, hence it can only be decrypted using destination node's private key to first decrypt the session key and using it decrypt the data. Even if the public key is known to intruders, it cannot be used to decrypt the packet. We choose to use asymmetric key cryptography over symmetric key cryptography because network nodes have enough resources, battery and computational power to compute complex encryption/decryption. This introduces technical challenges for the intruder to break the encrypted data packets. This also avoids repeated rekeying process and reduce communication overhead.

Proposed Secure-GLOR method is secured against any kind of malicious attack as we use different keys for encryption and decryption process. Finally, we conclude that intruder cannot predict the keys to read the data packets.

6. Simulation and Results

As discussed in the previous paper [7] the GLOR protocol has been developed in Visual Studio using C#. The machine used for simulation is powered by a 6th Gen. Intel i7 (3.1 GHz) CPU and 16GB DDR3L RAM running Windows 10.

6.1 Environment Setup

The environment consists of nodes evenly spread on a 2D plane. The nodes location is calculated using the X-Y coordinate of the device on the 2D plane. The web register is implemented using a local database. The nodes have been allocated random transmission speeds varying from 11Mbps to 25Mbps based on which the transmission time is calculated.

As the aim is to test absolute performance of different encryption algorithms using the same conditions, the test-bed includes the following assumptions

- The nodes have already been authenticated and have a unique id.
- None of the nodes fail during the operation.
- All nodes have the capability to calculate their location.
- No packet is dropped during the transmission process.
- Each node has a direct/indirect connection to the web register.

6.2 Simulation and Observation

The simulation initiates with the nodes calculating their geo location (using their X-Y coordinates) and generate a Public-Private Key pair for session key encryption and a randon session key for data encryption. The nodes send their location and public key to the web register and start connecting to the neighbor nodes to create the neighbor table to improve network performance.

The nodes use a predefined data-set to be communicated between the source and destination nodes. There are 72 nodes being used in this setup and information like transmission time, CPU utilization, and memory utilization is calculated and compared with various encryption schemes. This provides us with valuable information about how the network performs under different scenarios.

6.3 Results and Analysis

In the initial testing [21], without using hybrid encryption results were calculated for both symmetric and asymmetric encryption techniques individually. The same constants were then used to implement the hybrid encryption. This section presents and compares the results from the hybrid encryption techniques.

As discussed above, the hybrid encryption technique uses a combination of symmetric and asymmetric encryption schemes. The symmetric encryption technique is used to encrypt the data using a session key, whereas the asymmetric encryption technique is used to encrypt the session key using the public key of the destination node.

We have considered the following encryption techniques based on their individual strength and performance. We evaluated AES 128, AES 256 and Blowfish which for the data encryption while in combination with RSA 1024, RSA 2048 and Elliptic Curve Diffie Hellman (ECDH) for session key encryption. The combination of symmetric and asymmetric techniques used have been referred to as “case” and are listed as follows:

Table 2: Hybrid Encryption Scenarios

Case	Symmetric Encryption	Asymmetric Encryption
0	None	None
1	AES 128	RSA 1024
2	AES 128	RSA 2048
3	AES 128	ECDH
4	AES 256	RSA 1024
5	AES 256	RSA 2048
6	AES 256	ECDH
7	Blowfish	RSA 1024
8	Blowfish	RSA 2048
9	Blowfish	ECDH

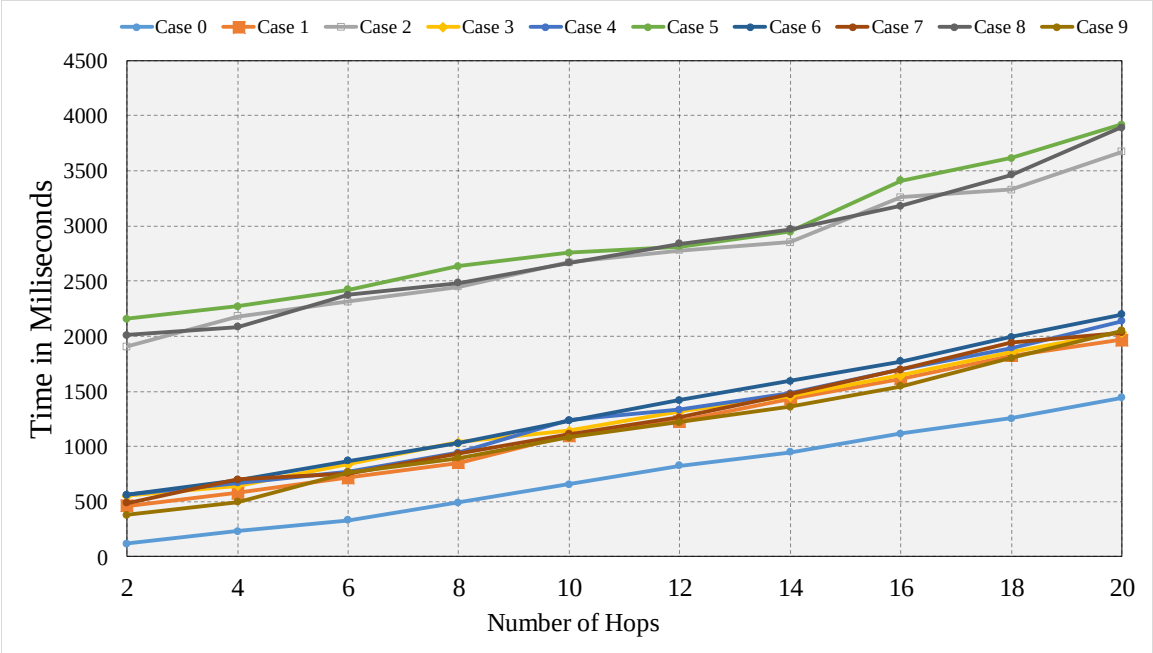

Fig. 8. Time taken for trip (500-Bytes data)

Fig. 8 and Fig. 9, give us a network performance insight in respect to the time taken for a data packet to be created, sent to the destination and receive an acknowledgement for the same. It also shows us the amount of delay obtained in proportion to the distance travelled. As the constraints are kept exactly as before, we take a 500-byte data-set for the first setup (Scenario 1) and a 64000-byte data-set for the second setup (Scenario 2).

For Scenario 1, using a 500 bytes data-set, it is observable form the data presented in Fig. 8 that hybrid encryption techniques using RSA 2048 (Case 2, 5 & 8) take upto 2000 milliseconds extra as compared to the RSA 1024 or ECDH for secret key encryption. Another closer observation also tells us that the hybrid encryption techniques using AES 256 (Case 4, 5 & 6) take slightly more time to encrypt the data as compared to AES 128 of Blowfish. In general, a gradual increase in time is expected with a direct relation to increase in number of hops a packet must travel before completing a round-trip.

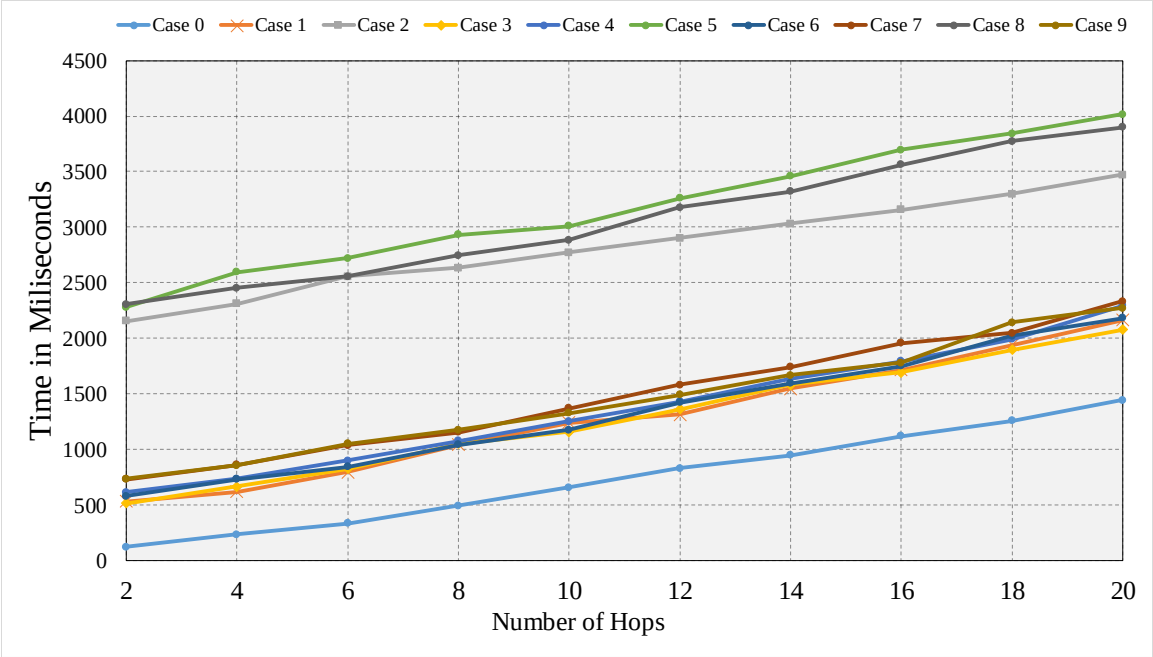

Fig. 9. Time taken for trip (64000-Bytes data)

When re-running the simulation for Scenario 2 with a data set of 64000 Bytes data-set, the results obtained show an increase of approximately 250 milliseconds for all cases as compared to Scenario 1. This upward shift is directly proportional to the size of data being encrypted and sent over the network. A gradual increase in time is once again expected with a direct relation to increase in number of hops similar to Scenario 1.

Other observations such as the increased 2000 milliseconds it takes for RSA 2048 as compared to RSA 1024 or ECDH and approximate incremental of 250 milliseconds for AES 256 as compared to AES 128 of Blowfish is also similar in both Scenario 1 and Scenario 2. Overall the data from both Scenarios can be majorly classified on the basis of hybrid encryption using RSA 2048 and hybrid encryption using RSA 1024 / ECDH due to the huge difference.

As just the time parameter is not enough to select a preferred combination of symmetric and asymmetric encryption technique, we also take into account the performance of the encryption techniques by measuring the resources used. The performance analysis is another major factor deciding how much resource consumption is adequate for the network model. Fig. 10 displays the Memory (RAM) consumption and Fig. 11 displays the CPU utilization for the various cases discussed above.

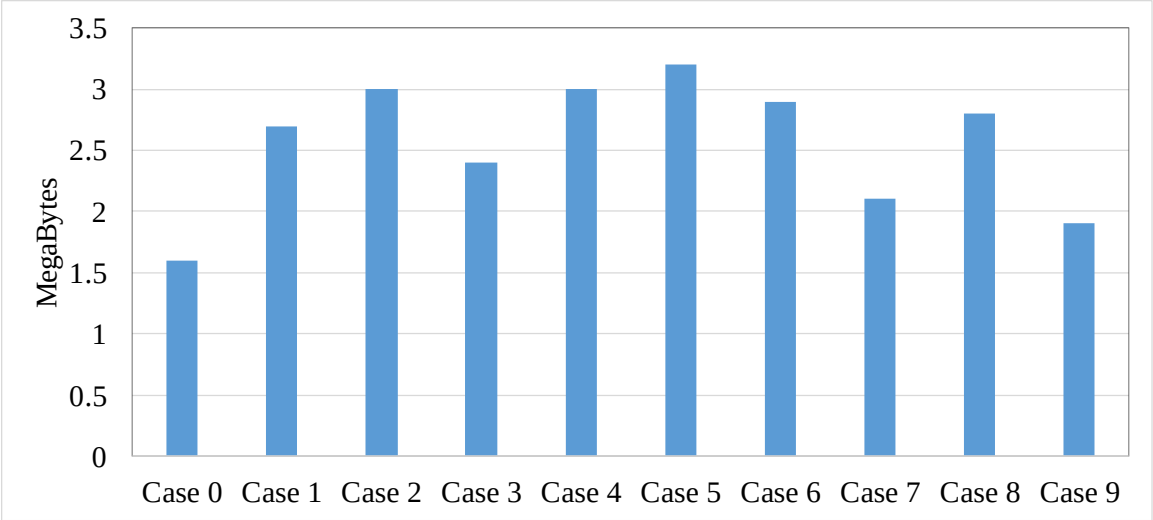

Fig. 10. Memory consumption.

From Fig. 10 we can observe that the hybrid encryption using AES 256 has the highest RAM consumption for data encryption as compared to other symmetric encryption techniques. It can also be deduced that RAM consumption is also high when using RSA 2048 for session key encryption as compared to other asymmetric encryption techniques. Fig. 11 also presents similar results for maximum CPU consumption by the RSA 2048 when encryption the session keys. However, the highest CPU consumption for encryption the data is AES 128, which is unlike the previous observation.

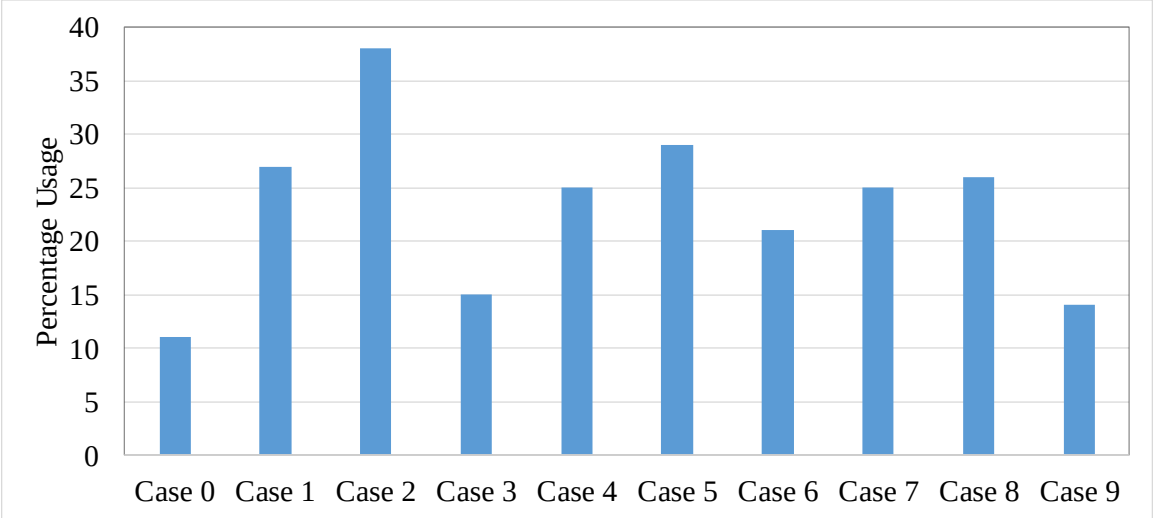

Fig. 11. CPU usage.

In conclusion, when compiling all the data received it is clear that Case 9 has the least resource consumption as well as one of the best performance amongst the compared symmetric and asymmetric encryptions techniques. Hence it seems promising to use Blowfish as the symmetric encryption technique for the encryption of data using the session key and for encrypting the session key Elliptic Curve Diffie Hellman (ECDH) would be the preferred asymmetric encryption technique.

7. Conclusion and Future Work

The results collected from the various combinations of symmetric encryption techniques and asymmetric encryption techniques were vital in deciding the preferred combination to use for the hybrid encryption model. The choice to use hybrid encryption also improves the performance of the network by reducing the load on the devices caused if only asymmetric encryption was used.

This is because of the fact that asymmetric encryption can only encrypt a certain amount of data at a time which is dependent on the size of the keys being used hence, multiple rounds of encryption is required to encrypt bigger sets of data. Hybrid encryption overcomes this issue by using symmetric encryption, a proven faster technique, to encrypt the data using a session key which in turn is encrypted by an asymmetric encryption technique.

In addition to the hybrid encryption technique, the Secure-GLOR also benefits from applying hybrid authentication scheme applied across network devices. This enables us to create a complete integrated security model for a mesh network. In our future works, we will address real world implementation of our scheme and develop dynamic key management strategy to defend against multiple attacks and threats.

8. Acknowledgments

The authors would like to acknowledge Pulkit Rohilla and Andrew Iskander for their contribution and technical assistance in implementation of Secure-GLOR model and setting up the various scenarios used in testing.

9. References

[1] J. Thomas, J. Robble, N. Modly, Off Grid communications with Android, IEEE Conference on Technologies for Homeland Security, 2012.

[2] P. Wong, V. Varikota, D. Nguyen, A. Abukmail, Automatic android-based wireless mesh networks, Informatica 38, no. 4 (2014) 313.

[3] P. Gardner-Stephen, The serval project: Practical wireless ad-hoc mobile telecommunications, Flinders University, Adelaide, South Australia, Tech. Rep (2011).

[4] Opengarden, https://opengarden.com (Accessed: 19-May-2015).

[5] M. Rogers, E. Saitta, B. Tyers, The briar project, https://code.briarproject.org (Accessed: 1-June-2015)

[6] M. S. Siddiqui, Security issues in wireless mesh networks, IEEE International Conference on Multimedia and Ubiquitous Engineering, 2017, pp. 717-722.

[7] A. Nanda, P. Nanda, X. He, Geo-Location Oriented Routing Protocol for Smart Dynamic Mesh Network, IEEE 18th International Conference on High Performance Computing and Communications, 2016, pp. 891-898.

[8] A. Nanda, P. Nanda, X. He, A. Jamdagni, A Secure Routing Scheme for Wireless Mesh Networks, 12th International Conference on Information Systems Security, 2016, vol. 10063, p. 393.

[9] P. Gallagher, Digital signature standard (dss), Federal Information Processing Standards Publications, volume FIPS (2013): 186-3.

[10] P. Zimmermann, A proposed standard format for RSA cryptosystems, IEEE Computer 19, no. 9 (1986): 21-34.

[11] NIST FIPS, 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/NIST, 2001.

[12] S. Heron, Advanced Encryption Standard (AES), Network Security, 2009(12), pp. 8-12,

[13] D. Puthal, S. Nepal, R. Ranjan, J. Chen, DLSeF: A Dynamic Key Length based Efficient Real-Time Security Verification Model for Big Data Stream, ACM Transactions on Embedded Computing Systems, Vol. 16(2), 2017.

[14] D. Puthal, X. Wu, S. Nepal, R. Ranjan, J. Chen, SEEN: A Selective Encryption Method to Ensure Confidentiality for Big Sensing Data Streams, IEEE Transactions on Big Data, 2017.

[15] D. Puthal, S. Nepal, R. Ranjan, J. Chen, A Synchronized Shared Key Generation Method for Maintaining End-to-End Security of Big Data Streams, 50th Hawaii International Conference on System Sciences, 2017, pp. 6011-6020.

[16] D. Puthal, S. Nepal, R. Ranjan, J. Chen, Threats to Networking Cloud and Edge Datacenters in the Internet of Things, IEEE Cloud Computing. Vol. 3(3) , 2016, pp. 64-71.

[17] D. Puthal, S. Mohanty, P. Nanda, U. Choppali, Building Security Perimeters to Protect Network Systems against Cyber Threats, IEEE Consumer Electronics Magazine, 2017.

[18] A. Rasheed, et. all, Private matching and set intersection computation in multi-agent and industrial control systems, 12th Annual Conference on Cyber and Information Security Research, 2017, p. 14.

[19] O. Cheikhrouhou, M. Laurent-Maknavicius H. Chaouchi, Security architecture in a multi-hop mesh network, 5th Conference on Security and Network Architectures, 2006.

[20] A. Ramesh, A. Suruliandi, Performance analysis of encryption algorithms for Information Security, IEEE International Conference on Circuits, Power and Computing Technologies, 2013.

[21] A. Nanda, P. Nanda, X. He, A. Jamdagni, D. Puthal, Secure-GLOR: An Adaptive Secure Routing Protocol for Dynamic Wireless Mesh Networks, 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2017, pp. 269-276.

[22] A. Nanda, P. Nanda, X. He, A. Jamdagni, D. Puthal, A Novel Hybrid Authentication Model for Geo Location Oriented Routing in Dynamic Wireless Mesh Networks, 51st Hawaii International Conference on System Sciences, 2018, In Press.