Secure-GLOR: An Adaptive Secure Routing Protocol for Dynamic Wireless Mesh Networks

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*— With the dawn of a new era, digital security has become one of the most essential part of any network. Be it a physical network, virtual network or social network, the demand for secure data transmission is ever increasing. Wireless mesh networks also stand the same test of security as the legacy networks. This paper presents a secure version of the Geo-Location Oriented Routing (GLOR) protocol for wireless mesh networks, incorporating a multilevel security framework. It implements authentication using the new features of the network model and enables encryption throughout the network to provide high levels of security.**

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

I. INTRODUCTION

As the world progresses to new technologies, we become more reliant on our technical advancements to handle our day to day data. This dependency is now raising concerns about the security of the millions of bytes of data being transmitted all over the world every day.

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, the data is accessed by more than just the device it was destined for. Hence a need for securely delivery of data is very critical to the future of such network model [6].

This paper presents the secure version of the GLOR protocol, as proposed in the previous paper [8]. Section II of this paper begins with a discussion about related approaches/models and how they implement security. Section III 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 IV followed by a theoretical analysis of the model in Section V. Section VI presents the performance of the network model under different scenarios with various configurations and discusses the results obtained. Finally, Section VII concludes with the final thoughts on the next step of GLOR protocol.

II. 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 are there in wireless communication networks, the layer wise classification of the security threats and solutions are given in [17][18]. In [13][14], it is already proved that symmetric key solutions

are thousand times faster than a symmetric key solution. Symmetric key cryptography is always suitable for the low power devices, where shared key need to be updated after certain period of time [13][14][15]. Current research trend creates hybrid architecture by combining communication and computing technologies such as fog or cloud computing. In [16][19][20], authors have given the novel security solutions for these hybrid architectures. Cheikhrouhou et al. [21] 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.

III. GEO-LOCATION ORIENTED ROUTING (GLOR)

Geo Location Oriented Routing (GLOR) [7] 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.

1) 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.

2) New Addressing Scheme:

The smart approach uses geo-location of a device as its IP address (described in Section III A). 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.

3) 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 III B).

4) Security Model:

The network model also implements authentication and encryption to improve the security of the network. The Model is further explained in Section IV.

A basic scenario of the protocol components and its working is defined in Fig. 1. The various components are defined in Table 1.

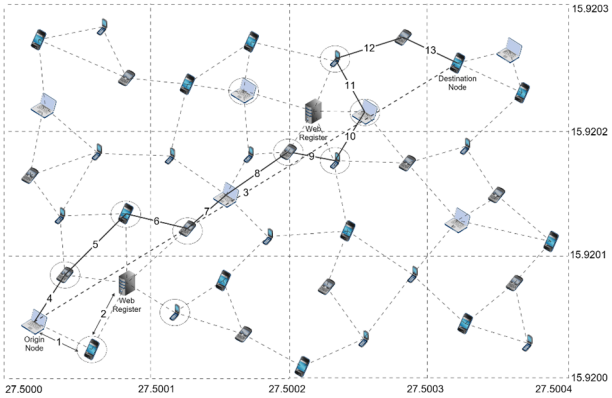

FIG. 1. DIFFERENT STEPS OF ROUTING PROCESS

TABLE 1. COMPONENTS OF GLOR PROTOCOL.

Component	Definition
Node	An electronic device (e.g. Smart-Phone, Laptop, and Tablet) that implements Geo-Location Oriented Routing (GLOR).
Normal Node	A node which has the capability to connect to other devices wirelessly and implements GLOR protocol.
Web Node	A Normal Node with the capability to connect directly to the Web Register.
Neighbor Node	A node X is said to be the neighbor node of Y if there exists a link between the node X and node Y.
Node Location	It is the Geo-Location of the Node, i.e. its latitude and longitude up to 4 decimal places and the node's Unique ID
Unique ID	The Unique ID of the node is a onetime generated Unique Identification number assigned to the Node alongside its MAC address during its first registration on the network.
Web Register	A cloud-based database dedicated for storing vital information about nodes, including their MAC address, unique ID, address, and current state.
Sector	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.

A. Node Addressing

GLOR protocol uses Geo Location as the IP address for the nodes. It is achieved by using the IPv6 addressing format that uses 32 hexadecimal bits. These are divided 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).

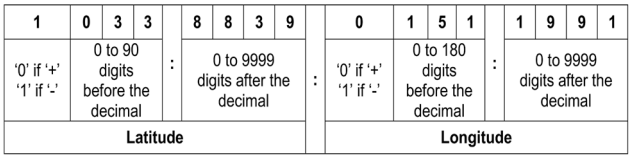

FIG. 2. ADDRESSING SCHEME (PART 1)

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.

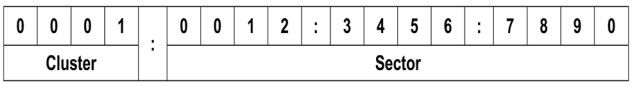

FIG. 3. ADDRESSING SCHEME (PART 2)

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

B. *Smart Packets*

GLOR 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 path.

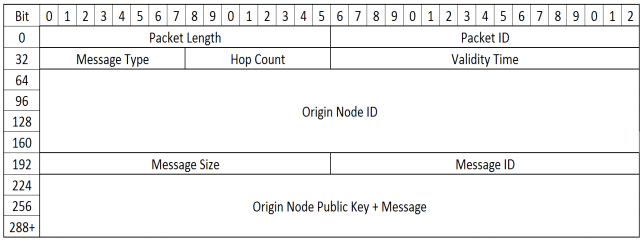

FIG. 4. PACKET FORMAT (OMITTING TCP/IP HEADERS)

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 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 it is updated each time to the address on the intermediate node.
- 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.
- 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.

C. *Web Register*

As referred to in Table 1, 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 neighboring 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 neighboring sector. In comparison to simple broadcast method, the sector-broadcast helps lower the load on the network.

D. *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.

IV. 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.

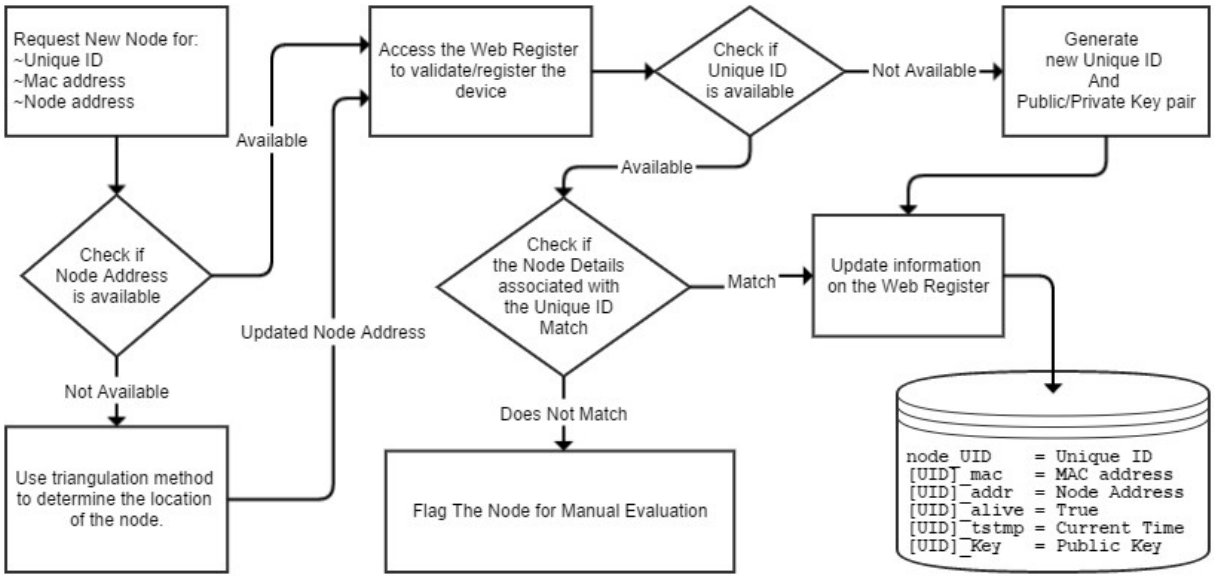

FIG. 5. NODE REGISTRATION PROCESS.

A. Authentication

It is the first step of security, a request to connect to the network and initiates the node registration process as shown in Fig. 5. The authenticated devices in the network collect information from a device that wishes to connect to the network. This data is first analysed by the authenticated node itself, compared with the data collected by its neighbour nodes from the device and then sent to the web register for further analysis.

The web register checks its database to find any records matching with the device information. If a record is found, it is compared to the device data in order to spot any spam nodes. Once the device is verified, it is given the 'authenticated node' status and all data to and from the device is hereafter encrypted until it disconnects from the network.

If the web register does not contain any records matching the device, it is considered to be a new device. In such case, the new device is requested to follow a one-time manual registration process that includes providing device details, selecting a unique ID and generating a Public-Private key to be used for encryption. The details (except the private key) are then sent to the web register and converted into a record and the new device is given the 'authenticated node' status and all data to and from the device is hereafter encrypted until it disconnects from the network.

Another important part of authentication is the monitoring of the network conducted by the web register. As it receives constant updates from nodes in the network including the change in geo-location, it can easily spot discrepancies in the data. For instance, if a device is trying to impersonate a node on the network, the web register would receive two sets of updates for the same device showing inconsistent data and hence flag the suspicion for further analysis.

It can also help identify lost or stolen devices once they try to reconnect to the network. The device data will be used to identify the node and its geo location can be used to recover it.

B. Encryption

Securing the data being transmitted through the nodes is another major factor for the integrity of network model. This is achieved by using asymmetric encryption throughout the network. As mentioned earlier, once a node has been authenticated all the data to and from the node is encrypted.

The encryption technique used is 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 - sender node; DN - destination node

1. At initial node registration

$\forall$ 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 III(D), 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.

V. THEORETICAL ANALYSIS

This section provides a theoretical analysis of our proposed Secure-GLOR model to show the working model with potential security threats and how Secure-GLOR is protected against them. We use asymmetric key cryptography to protect data in dynamic mesh network. The proposed security method performs efficiently without degrading network performance.

We have made a practical and realistic assumption in our method, as described below.

Assumption 1. In our method, the data that is encrypted by an asymmetric-key method cannot be decrypted by any other, unless they have the private key.

A. 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 maintain 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. Our network model uses high end resource devices (i.e. smartphones, laptop, etc.), so 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 use public key (K_{PU}) to encrypt and private key (K_{PR}) to decrypt the data packets, and each node only shares its public key with web register. Hence, an intruder can reach at 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 data packet using own private key (K_{PR}). 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.

B. Forward secrecy

By following a standard asymmetric key cryptography procedures, destination node's public key is used to encrypt the data packets, which can only be decrypted using destination node's private key. 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.

VI. 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.

A. 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.

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.

B. 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 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.

C. Results and Analysis

Fig. 6 and Fig. 7, 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.

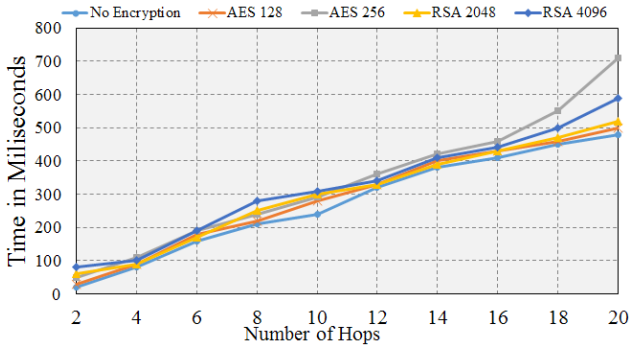

Fig. 6. Time taken for trip (500-Bytes data)

The comparison consists of both symmetric encryption (AES 128, AES 256) and asymmetric encryption (RSA 2048, RSA 4096). In the first scenario, a data-set of 500 Bytes is encrypted and sent from the origin node to the destination node. From Fig. 6, it is observed that there is steady increase in the time taken for the packet to reach its destination and it is directly proportional to the distance travelled (number of hops).

The graph also shows that there is very little difference in the time taken by AES 128 and RSA 2014, however AES 256 and RSA 4096 take a comparatively longer time due to the increased size of encrypted data. This implies that the network is able to perform normally even after encryption is used and does not cause any overhead/overload on the devices.

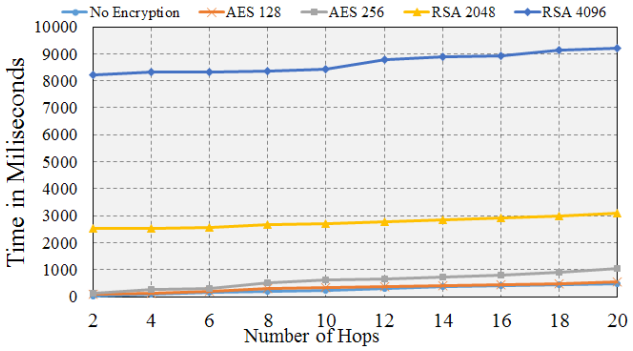

Fig. 7. Time taken for trip (64000-Bytes data)

In the second scenario, a data-set of 64000 Bytes is used to test the simulation. The results, as shown in Fig. 7, depict that the symmetric encryption has a similar steady increase comparable to scenario one. However, the asymmetric encryption has a very large increase (almost 2 seconds for RSA 2048 and 8 seconds for RSA 4069).

The major factor for such a high increase can be directly related to the key size for RSA encryption, which requires the data to be broken down into small chunks and then encrypted individually. This leads to a longer wait cycle during encryption and decryption process (at the origin and destination node).

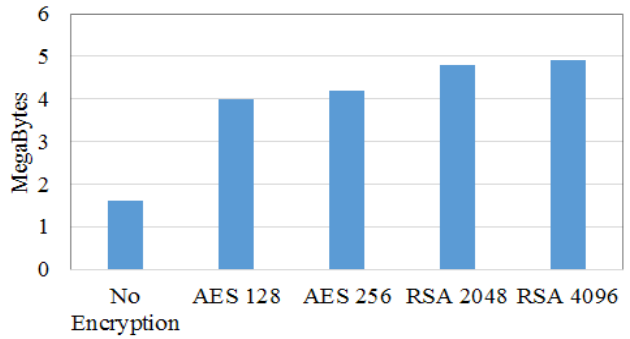

FIG. 8. MEMORY CONSUMPTION.

The performance analysis of each encryption technique based on resource consumption was also carried out in the above-mentioned scenario one and two. As Fig. 8 and Fig. 9 show us, the symmetric encryption techniques had similar memory consumption of about 4 Megabytes, however AES 256 had almost double CPU usage of 24 % as compared to AES 128 which only required 14%. Hence it can be deduced that even though the time required for both techniques is almost identical, the resource requirement for AES 256 is much more.

The asymmetric encryption techniques RSA 2048 and RSA 4096 had similar memory consumption (4.8 Megabytes) and CPU usage (27%-28%). Hence both techniques require almost the same amount of resources but their time consumption is directly proportional to the amount of data. However, overall the symmetric encryption had less resource consumption when compared to asymmetric encryption.

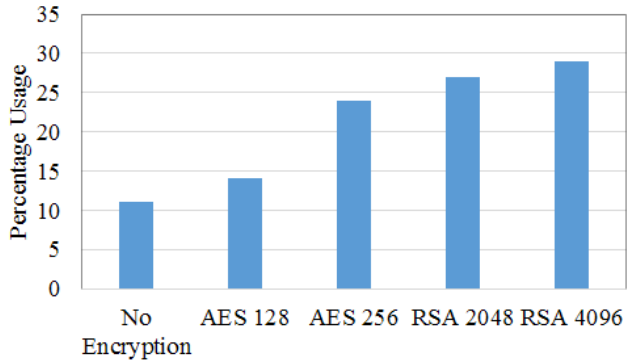

FIG. 9. CPU USAGE.

VII. CONCLUSION AND FUTURE WORK

The future challenge consists of finding ways to decrease the time taken in encryption and decryption process without increasing the resource requirement. One of the ways this can be achieved is by using hybrid encryption techniques that merges the best of both symmetric and asymmetric encryption techniques.

The results from the simulation provide a very vivid profile of all the encryption techniques that have been compared. It can be deduced that both symmetric and asymmetric encryption technique have similar performance results with a small data set however if the size of the data set is increased, the asymmetric encryption techniques require a lot more time and resources to perform the task.

Even so, the asymmetric encryption technique is more suitable to the GLOR protocol as the network model can provide more security by using public-private keys unique to each device as compared to a universal key for symmetric encryption.

VIII. ACKNOWLEDGMENTS

The authors would like to acknowledge Pulkit Rohilla for his contribution and technical assistance in implementation of GLOR protocol and setting up the scenario.

REFERENCES

[1] J. Thomas, J. Robble, and N.Modly. "Off Grid communications with Android." In 2012 IEEE Conference on Technologies for Homeland Security (HST). 2012.

[2] P. Wong, V. Varikota, D. Nguyen, and 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'. [Online]. Available: https://opengarden.com. [Accessed : 19-May-2015].

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

[6] M. S. Siddiqui. "Security issues in wireless mesh networks." In 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07), pp. 717-722. IEEE, 2007.

[7] A. Nanda, P. Nanda, and X. He. "Geo-Location Oriented Routing Protocol for Smart Dynamic Mesh Network." In High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on, pp. 891-898. IEEE, 2016.

[8] A. Nanda, P. Nanda, X. He, and A. Jamdagni. "A Secure Routing Scheme for Wireless Mesh Networks." In Information Systems Security: 12th International Conference, ICISS 2016, Jaipur, India, December 16-20, 2016, Proceedings, vol. 10063, p. 393. Springer, 2016.

[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, November 26, 2001.

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

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

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

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

[18] D. Puthal. "Secure data collection and critical data transmission technique in mobile sink wireless sensor networks." M.Tech Thesis, National Institute of Technology, Rourkela, 2012.

[19] D. Puthal, S. Nepal, R. Ranjan, and J. Chen. "A Secure Big Data Stream Analytics Framework for Disaster Management on the Cloud." in 18th IEEE International Conferences on High Performance Computing and Communications (HPCC 2016), pp. 1218-1225, 2016.

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

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