A Novel Hybrid Authentication Model for Geo Location Oriented Routing in Dynamic Wireless Mesh Networks

Ashish Nanda[1], Priyadarsi Nanda[1], Xiangjian He[1], Aruna Jamdagni[2], and Deepak Puthal[1]
[1]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

Authentication is an essential part of any network and plays a pivotal role in ensuring the security of a network by preventing unauthorised devices/users access to the network. As dynamic wireless mesh networks are evolving and being accepted in various fields, there is a strong need to improve the security of the network. It's features like self-organizing and self-healing make it great but get undermined when rigid authentication schemes are used. We propose a hybrid authentication scheme for such dynamic mesh networks under three specified scenarios; full authentication, quick authentication and new node authentication. The proposed schemes are applied on our previous works on dynamic mesh routing protocol, Geo location Oriented Routing Protocol (GLOR Simulation results show our proposed scheme is efficient in terms of resource utilization as well as defending against security threats.

1. Introduction

The mesh networks have evolved a great length in the past few years and are being used extensively for device to device communication. They feature a self-sustained network model where the data is transmitted from one point to other by the concept of hopping. This is achieved by connecting multiple devices together and then sending the data from the host device to the next device and repeating this process multiple times until the data finally reaches the destination node. This can be achieved through unicast/multicast routing where a single or multiple path is used to send data or by flooding the whole network with the data.

A typical mesh network can be either static or dynamic, depending upon the type of connected devices. If stationary/fixed devices form the mesh network, it is known as a static mesh network. It can be wired, wireless or a combination of both depending upon how devices connect to each other.

However, the dynamic mesh network is formed by mobile/portable devices but at the same time supports static devices as well. As the major part of the network consists of mobile/portable devices, all the devices use wireless communication to connect to each other. Hence it is known as the dynamic wireless mesh network and is a great platform for high performance devices such as smartphones, laptops, tablets, etc.

The dynamic wireless mesh network is a recent network type, which along with all the great features of mesh networks also provides a potential to expand easily. With a new network model custom-tailored for it, the dynamic wireless mesh network can start as a backup communication network that can work without any expensive infrastructure and someday may become a primary communication network.

The mesh network comprises of various noble features such as self-configuration, which allows the devices to connect and create the network without any external control entity. It involves low operating costs as the network is composed of user devices, which are easily, setup by implementing an identical protocol on all devices. The maintenance of the network can be considered by the device owners while providing robustness as multiple devices create redundant connections. A dynamic size can adapt according to the number of devices. In addition, the self-healing properties also make wireless mesh networks ideal network choice for future.

However, it is important to note that, mesh network sometimes is unable to perform at its full potential as the current/legacy protocols limit the extent of its features and size [1]. Aspects such as IP addressing requires a central server to manage the network which makes the network dependent on the server destroying its self-configuration properties [2].

As the mesh network works by sending data through multiple devices, these devices have access to the data flowing through the network [3]. This raises

URI: http://hdl.handle.net/10125/50579
ISBN: 978-0-9981331-1-9

various security concerns as the network becomes prone to even the simplest attacks such as eavesdropping which can compromise the privacy of the users and the integrity of the network.

Hence, along with various other network models, security has also become a must for mesh networks too. Recently, various security models have been developed for the mesh network [1 - 22], however the security models themselves have become another factor prevents the mesh to expand. To provide high levels of security, a central controller is used to manage the network, which indecently prevents the network from expanding and working at its true potential.

In this paper, we present various related/existing security schemes, how they implement authentication and their limitations in Section 2.1. Section 2.2 defines the problem statement whilst providing a summary on the main challenges. Following that, the paper presents briefly the Geo Location Oriented Routing (GLOR) protocol and its current authentications scheme in Section 3 and explains how we incorporate its new features for the lightweight hybrid authentication model. Section 4 presents our proposed authentication scheme with various scenarios and how they work to provide better security. Section 5 presents the simulation results and analysis and finally, we conclude the paper in Section 6.

2. Related Works and Problem Statement

The wireless mesh network is prone to various types of threats ranging from basic attacks like Denial of Service, Eavesdropping, Spoofing, Flooding, etc., all the way to much advanced attacks such as the Sinkhole attack, Impersonation, Sybil attack, data redirect, and many more [1,13]. In essence, most of the attacks in mesh networks can be traced to a compromised device or an unauthorised access to the network. Hence authentication plays a crucial and integral part preserving security of the network by keeping the attackers away from accessing the network.

2.1. Related works

The wireless mesh network has some well-known routing techniques such as the OLSR (Optimized Link State Routing) [8, 9, 10] and AODV (Ad hoc On-Demand Distance Vector) [12], both these schemes have almost no security aspect by themselves but, lately they have been modified to include security. SOLSR is a secure version of the OLSR protocol which uses features like message authentication codes (MAC's), timestamping and cryptographic signatures to prevent the most common attacks on OSLR such as identity spoofing, link spoofing, tc packet spoofing [14].

Similarly, SAODV is a secure version of AODV protocol which implements two mechanisms, digital signatures [4] and hash chains, to provide security and ensure the integrity of the network [15]. There are various other protocols such as ARAN (Authenticate Routing for Ad hoc Networks), which uses a single trusted key pair for the whole network to ensure security [16]. SRP (Secure Routing Protocol) [17], SMT (Secure Message Transmission Protocol) [19] and SAR (Security-Aware Ad Hoc Routing Protocol) [20] use shared secret key amongst devices to verify packets. Protocols like SEAD (Secure Efficient Ad Hoc Distance Vector Routing Protocol) [18] and SLSP (Secure Link State Routing Protocol) [21] use table-driven approach along with time-synchronization or secret key exchange and other similar featured protocols.

However, most security schemes are either based on flooding technique, which increases the network load on each device, or they require an existing security association between the devices. Others such as OLSR are known to self-saturate the network just by overcrowding of Hello messages.

Hybrid Authentication is a must for multihop networks as it can provide redundant ways in which a device can authenticate itself or other devices [24, 25]. It is also certain that there is a need for an authentication server to verify and keep a check on all the authentications. At the same time, there must exist other equally secure ways of authentication so that the network can function even if the authentication server is unreachable [26, 27]. A similar approach that implements hybrid authentication is presented in [22] which, discusses a multi-level model for authentication. However, the model can only be applied to static wireless mesh networks and not the dynamic wireless mesh networks.

2.2. Problem Statement

The dynamic wireless mesh network requires a dynamic security model comprising of a new authentication scheme, which can adapt to various scenarios and still be able to provide high levels of security. As it is made up of mobile devices, which keep switching connections as they move, a static authentication scheme with rigid rules will slow down the network.

In addition, a mobile device in the network might not always have access to the authentication server and will be unable to gain network access which will lead

to a limited/fixed sized network, preventing its expansion and network coverage.

3. The GLOR routing model

In our previous effort, we have developed the Geo Location Oriented Routing (GLOR) protocol [2], which is more suited for dynamic wireless mesh networks [2]. The network model also provides a set of new features that can be used to implement better security in the network. Some of the new features of the GLOR protocol are as follows:

Reverse Network Model: The devices that make up the mesh network are self-maintained and contribute resources to maintain the network as well removing the need of centralised control.

New Addressing Scheme: As the name of the protocol suggests, it uses geo-location as the address of a device in place of the IP address.

Smart Packets: As the protocol uses geo-location, a data packet equipped with the geo-location of its destination can dynamically find a path through the devices without mapping the whole network.

Security Model: The GLOR security model includes basic authentication, monitoring and an end-to-end encryption [23], which is achieved using asymmetric encryption (Public – Private key pair) [10].

Web Register: It is defined as the "yellow pages" of the GLOR network model and is responsible for storing information like mac address, unique ID, location, public encryption key, etc. for every registered device on the network. Its purpose is to keep records in the cloud that can be accessed for authentication purposes and to provide device location information for better routing efficiency.

Although the protocol provides an adequate authentication scheme, it does not take into account the various scenarios a new device can encounter during the authentication process. With all the above features, the GLOR protocol provides the required features and the platform to be suitable for a new dynamic authentication model. Hence, this paper builds upon the existing work done by the authors [2, 3, 23].

4. Authentication Mechanism

The GLOR model presents a basic authentication scheme [3], which is dependent on the web register for verification of the device details. However, getting access to the web register might not always be possible. This can result in a long delay for the new device to gain access to the network.

In addition, the authentication process requires the devices to first establish a connection to the network and is then authenticated which poses a security threat to the network itself.

In order to make the authentication process faster and much more secure, we propose three scenarios which encapsulate all possible conditions a device can encounter while establishing a connection to the network. During authentication, the new device is kept in a sandbox scenario, which prevents the new device to discover any further details about the network. The new device is not provided network access until the authentication is successful. The three distinct scenarios are described as following.

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.

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	RSA-2048 based encryption key pair used for authentication and End-to-End encryption. Each device gets its own key pair.
K_{PI}	Private Key	
K_{CR}	Crypto Key	AES-256 based encryption key provided to each device at registration.

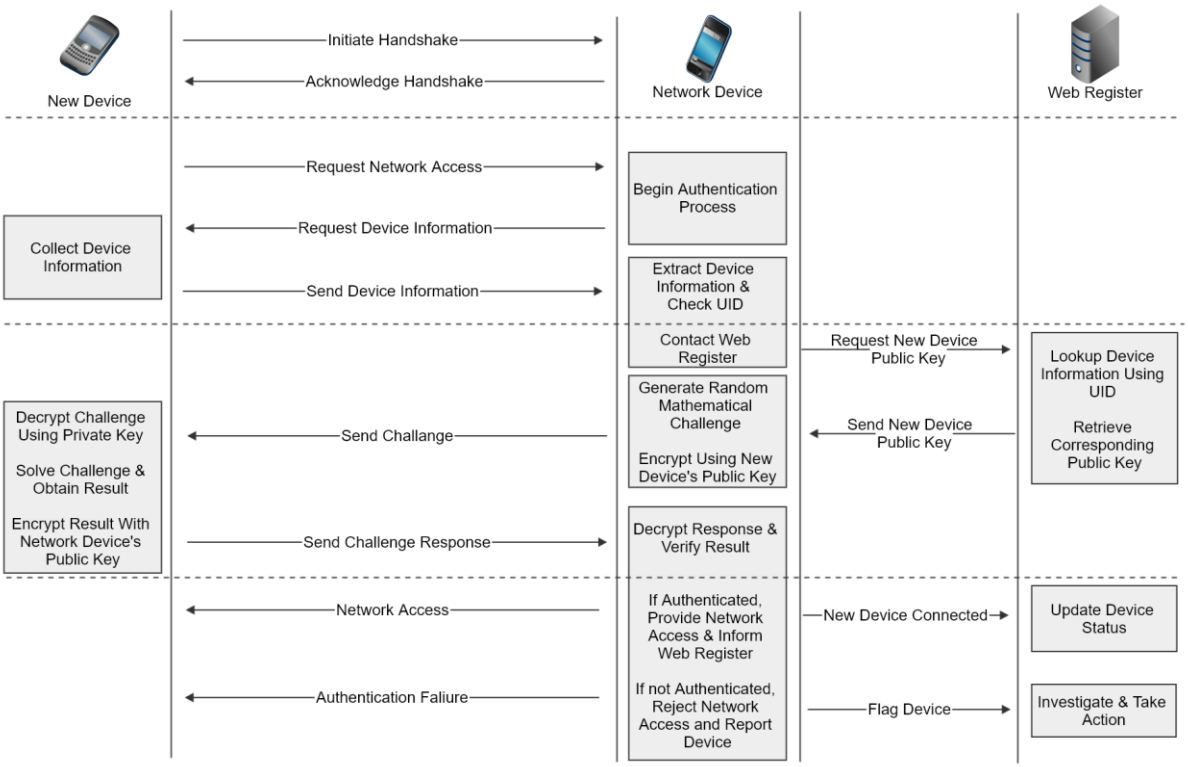

Fig. 2: Full Authentication Process

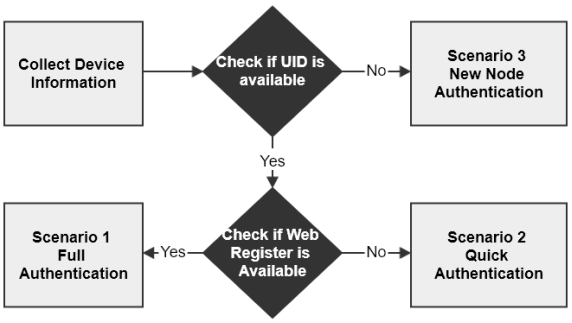

Fig. 1: Authentication Scenario Selection

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.

Once the Node has collected enough information about the Device, it decides upon the authentication scenario to be used. The decision on which scenario the device must pass through is based on the availability of; the new device's unique ID and access to the web register as shown in Fig. 1. The presence of UID implies that the new device has been registered and is re-connecting to the network.

Table 1 lists various components of the hybrid authentication model and associated terms used to represent them.

The authentication scheme is based on 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) style device. Such device is then used to prevent any unauthorized access to the sensitive information if a device on the networks is internally compromised. The authentication scenarios are discussed in details below.

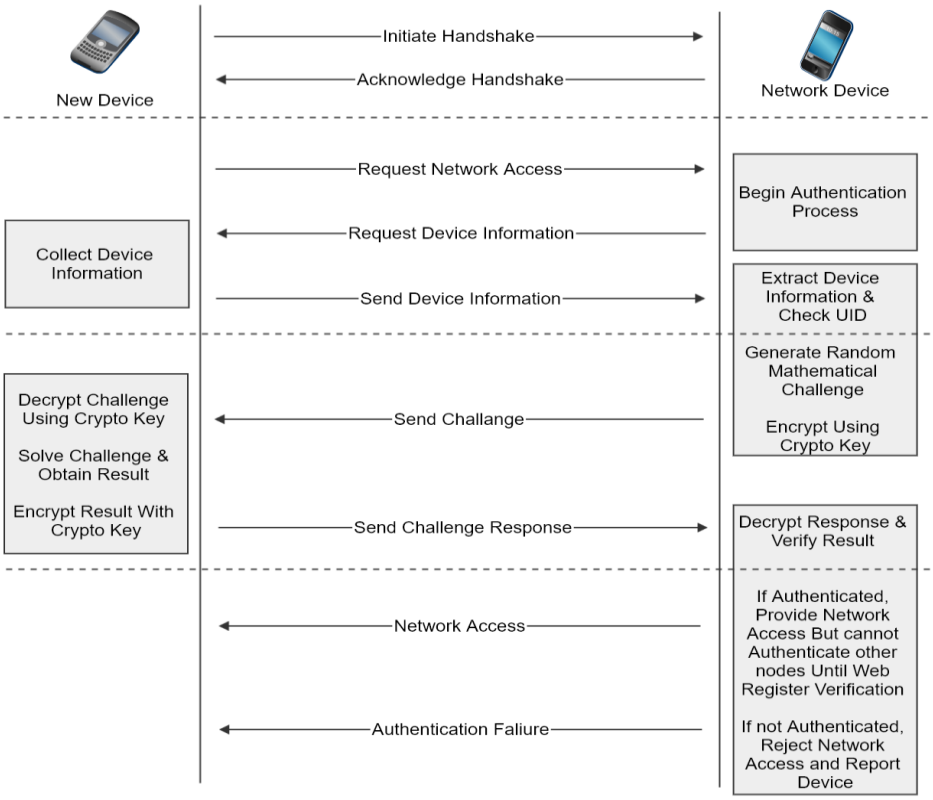

Fig. 3: Quick Authentication Process

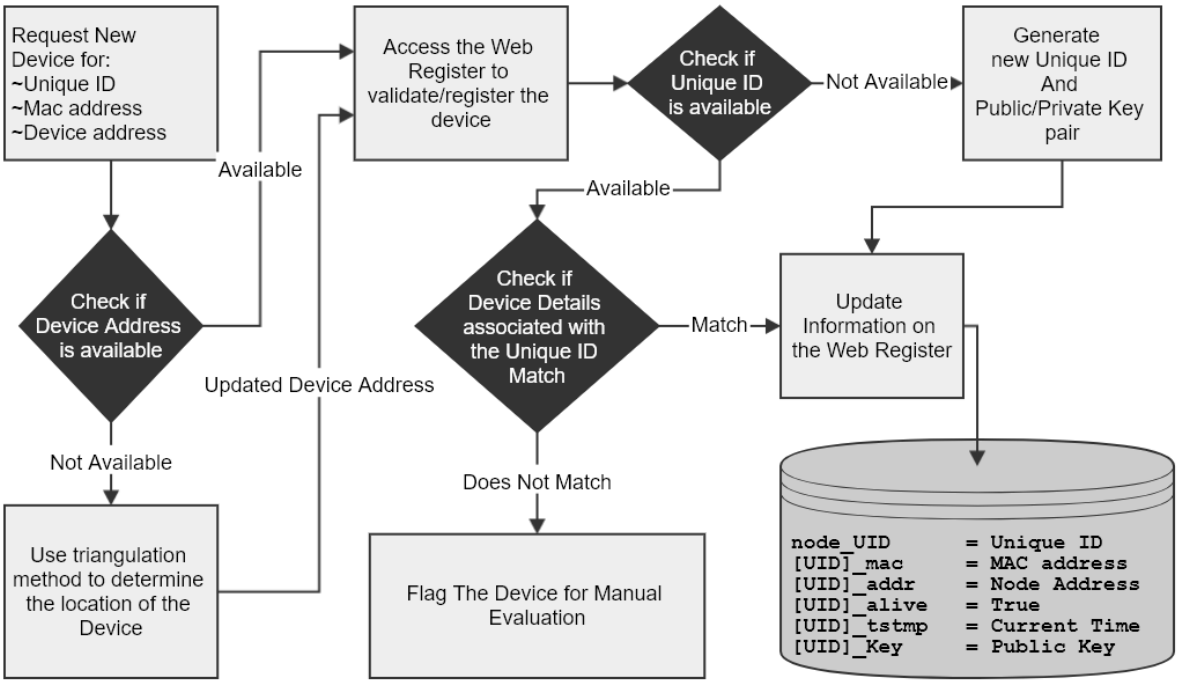

Fig. 4: Registration and New Node Authentication

4.1. Scenario 1 – Full Authentication

The steps in full authentication process are divided into four major parts: Handshake, Device Information Collection, Challenge and Decision as shown in Fig. 2. Individual processes are defined as follows.

Algorithm 1: Scenario-1 Challenge

$K_{PI}(D)$ - private key of D; $K_{PU}(D)$ - public key of D
VAR - Variable; OPR - Operator; RLT() – Result;
CLN - Challenge; RES – Response

1. Get device encryption key

Node requests WR for K_{PU}(Device)

Node (*Device(UID||MAC)*) → WR

If WR found Device in the register and verified

WR → Node: (K_{PU}*(Device)*)

2. Create challenge

Node uses random function to generate equation

Node(Random) = VAR_1, VAR_2 & OPR_1

Node checks if equation is valid

RLT(Node) = VAR_1 OPR VAR_2

If RLT(Computable) = True, Go To Step 3.

If RLT(Computable) = False, Repeat 2.

3. Send challenge

Node uses K_{PU}(Device) to encrypt challenge and add K_{PU}(Node)

CLN = K_{PU}(Device)[VAR_1 OPR VAR_2 || K_{PU}(Node)]

Node → Device: (CLN)

4. Solve response

Device uses K_{PI}(Device) to decrypt and solve challenge

K_{PI}(Device)[CLN] = VAR_1 OPR VAR_2 || K_{PU}(Node)

RLT = VAR_1 OPR VAR_2

Device uses K_{PU}(Node) to send the response

RES = K_{PU}(Node)[RLT]

Device → Node: (RES)

5. Verify response

Node extracts the response using K_{PI}(Node)

K_{PI}(Node)[RES] = RLT(Device)

If RLT(Node) == RLT(Device), Grant Net Access & Authentication Rights

Node (*Device(Connected)*) → WR

If RLT(Node) =! RLT(Device), Authentication Fail

Node (*Device(Flagged)*) → WR

Handshake: The very first step for the Device is to scan its surroundings for devices using the GLOR protocol. Once a Node (a device implementing the GLOR protocol and being connected to the network) is found, the Device will initiate a handshake request.

The Node will then respond to the request to complete the handshake. Once the Handshake is over, the Device requests the Node for network access, which then initiates the authentication process.

Device Information Collection: Before the authentication process begins, the Node must first request the Device for its information including details such as UID, MAC, ADDR, etc. The Device must then provide the above-mentioned information to the Node as these details play an important role in verifying the status of the device.

The Node will first check if the Device has a UID as it is only provided to registered devices. Once the presence of UID has been verified, the device information is forwarded to WR.

Algorithm 1 provides details on the creation and the process of challenge-response used in scenario 1.

Challenge: Once WR receives the Device's information, it looks for the device records in its own database by referring to the UID. Once the details are found, they are compared with the Device's details provided by the Node. If the details match, the Device is verified and web register sends the K_{PU}(Device) to the Node.

Upon receiving the K_{PU}(Device), the Node will then create a random mathematical challenge where both the values and the operation will be chosen at random (e.g. "10 ^ 4", "74 / 3 * 4", etc.). This challenge will then be encrypted using the K_{PU}(Device) and sent across to the Device ensuring that only the device that possesses the K_{PI}(Device) (Stored in the Trusted Platform Module) will be able to decrypt the challenge and solve it.

To ensure there is no intrusion during the process, the Node will also send along its own K_{PU}(Node) so that the challenge response is also encrypted. The Device can now use K_{PI}(Device) to decrypt the challenge, solve the equation and use the K_{PU}(Node) to encrypt the result and send the response back.

Decision: Upon receiving the response from the Device, the Node will decrypt the response with K_{PI}(Node) and check the result. Once the result is verified, the Node will finally provide network access to the Device along with the right to authenticate other devices on the behalf of the network. The Node will also send an update to the WR informing that the Device has gone through the authentication process and has been verified and provided network access.

The WR will update the ADDR and last seen information in its records for the Device and enable the right to authenticate. This will ensure no node can add another Device until it has been verified by the WR.

4.2. Scenario 2 – Quick Authentication

Like the full authentication process, the quick authentication process is also divided into four major

parts: Handshake, Device Information Collection, Challenge and Decision as shown in Fig. 3.

Handshake: This process is identical to the one used in the previous scenario.

Device Information Collection: Before the authentication process begins, the Node must first request the Device for its information which, includes details such as UID, MAC, ADDR, etc. The Device must then provide the above-mentioned information to the Node as these details play an important role in verifying the device.

The Node will first check if the Device has a UID as it is only provided to registered devices. Once the presence of UID has been verified, the device checks if it can access the WR.

Algorithm 2 presents the technical exchange that takes place during this authentication process.

Algorithm 2: Scenario-2 Challenge

K_{CR} - crypto key; VAR - Variable; OPR - Operator; RLT() - Result; CLN - Challenge; RES - Response

1. Create challenge

Node uses random function to generate equation

$$Node(Random) = VAR_1, VAR_2 \ \& \ OPR_1$$

Node checks if equation is valid

$$RLT(Node) = VAR_1 \ OPR \ VAR_2$$

If RLT(Computable) = True, Go To Step 2.

If RLT(Computable) = False, Repeat 1.

2. Send challenge

Node uses K_{CR} to encrypt challenge

$$CLN = K_{CR}[VAR_1 \ OPR \ VAR_2]$$

$$Node \rightarrow Device: (CLN)$$

3. Solve response

Device uses K_{CR} to decrypt and solve challenge

$$K_{CR}[CLN] = VAR_1 \ OPR \ VAR_2$$

$$RLT = VAR_1 \ OPR \ VAR_2$$

Device uses K_{CR} to send the response

$$RES = K_{CR}[RLT]$$

$$Device \rightarrow Node: (RES)$$

4. Verify response

Node extracts the response using K_{CR}

$$K_{CR}[RES] = RLT(Device)$$

If RLT(Node) == RLT(Device), Grant Net Access

Wait for Connection → WR

Node (*Device(UID||MAC||Connected)*) → WR

If RLT(Node) =! RLT(Device), Authentication Fail

Wait for Connection → WR

Node (*Device(UID||MAC||Flagged)*) → WR

Challenge: As the WR is not available or times out, the Node must follow the quick authentication process. As the Node cannot receive the K_{PU}(Device) from the WR, it uses the GLOR K_{CR} (a symmetric encryption key).

The Node will create a random mathematical challenge where both the values and the operation will be chosen at random (e.g. "10 ^ 4", "74 / 3 * 4", etc.). This challenge will then be encrypted using the K_{CR} and sent across to the Device, ensuring that once again only a registered device will be able to decrypt the challenge. This is possible because the K_{CR} is only provided to registered devices during their first registration and is stored in a Trusted Platform Module (which is known to be extremely secure) only to be accessed by the GLOR protocol for encryption and decryption purposes.

Decision: Upon receiving the response from the Device, the Node will decrypt the response with the K_{CR} and check the result. Once the result is verified, the Node will finally provide network access to the Device. However, the Node will not provide the right to authenticate other devices until a verification is done by the WR. The Node will now wait for an access to the WR and inform it once the connection is achieved and the Device is verified and connected.

The WR will check the device information against its records and if verified, it will provide the Device with the right to authenticate other Devices on the behalf of the network. The WR will also update the ADDR and last seen information in its records.

This scenario introduces a new K_{CR} (AES 256) [11,12] which, provides an alternate method for authentication if the WR is not available. The K_{CR} referred here as universal and is saved inside a trusted platform module (or a trusted execution environment for devices that do not possess the hardware). The K_{CR} can only be accessed by the GLOR protocol for encryption-decryption purposes in case no immediate access to the WR is available.

The Device can now use its K_{CR} to decrypt the challenge and solve it. Once solved the Device will again use K_{CR} to encrypt the result and send the response back to the Node.

4.3. Scenario 3 – New Node Authentication

In this scenario, we take into account the device that is connecting to the network for the first time hence; it does not have any UID. In addition, the WR will not also contain any record matching the Device's information. Hence, a new record will be created as shown in Fig. 4.

This scenario also incorporates the device registration process as defined by GLOR [2]. The new node authentication scenario is divided into four parts: Handshake, Device Information Collection, Verification and Registration.

Handshake: This process is identical to the one used in the previous scenario.

Device Information Collection: Similar to the previous scenarios, the Node first requests the Device for its information. The Device must provide the required information, however, unlike the first two scenarios, it would not contain any UID. On verifying that the Device does not possess a UID, the Node must begin the registration process on it's own.

Verification and Registration: Before the Device can register; the Node must setup a secure connection to the Device as well as the WR to verify the details provided. To do so, the Device is asked to generate a new key pair K_{PI}(Device) and K_{PU}(Device), from which the K_{PI}(Device) is submitted to the trusted module and the K_{PU}(Device) is shared with the Node. Once the communication is secured, the Node will send the data to the WR for verification.

The WR upon receiving the Device's information will check if any matching records exist to make sure duplicate records are not found. If no duplicate records are found, the WR will create a record for the Device and generate a UID to map the device's information. The WR will then send the registration details to the Node, which will pass it onto the Device.

Once this process is complete, the Device will be provided network access by the Node and also given the right to authenticate other devices on behalf of the network.

5. Simulation and Results

The simulation for the authentication model using 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 with 16GB DDR3L RAM running Windows 10.

5.1. Environment Setup

The environment consists of two Smart Devices (both implementing the GLOR protocol), one of which being part of the network (Node) and the other attempts to connect to the network (Device). The Web Register (WR) is implemented using a local SQL database. The Device and Node have been allocated a maximum transmission speed of 11Mbps, which is an average speed of transmission based on the oldest non-legacy hardware still in use (Wi-Fi or Bluetooth). The transmission and processing times are calculated based on the processing power and transmission speed of the devices.

For the simulation environment, we consider following assumptions:

- None of the devices fail during the operation
- Both devices have the capability to calculate its Geo-Location (ADDR)
- There is no data loss during transmission.
- For scenario 1, the Node has a direct connection to the WR

5.2. Results and Analysis

The simulation involves the Device starting the authentication process by initiating the handshake with the Node. The simulation then proceeds along as defined in the scenarios. The simulation does not involve Scenario 3 (New Node Authentication) as it is an extension of full authentication and hence, would have similar results.

Simulation is conducted separately for each scenario and collecting information on transmission time, CPU utilisation, and memory utilisation. This provides us with valuable information about how the network performs under different conditions.

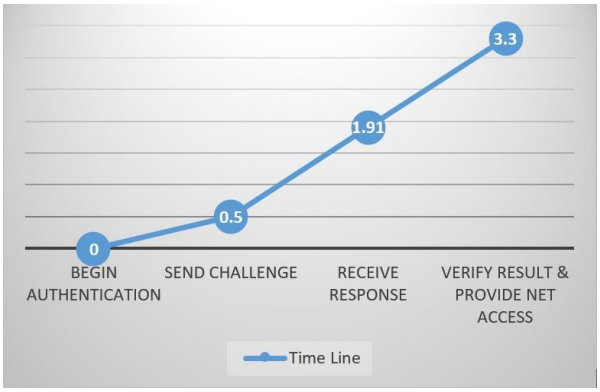

Fig. 5: Scenario 1 timeline

The simulation for Scenario 1 is conducted based on the model description from Section 3.1. The simulation starts with the devices authentication process. We then capture the time taken for the authentication process to complete. Fig. 5 displays a timeline of the authentication process starting at 0 seconds and finishing at 3.3 seconds while mapping the key tasks in between.

The authentication process begins once the handshake is completed and is denoted by '0' on the time scale in Fig. 5 & 6. Once the node has created the challenge it sends it to the device, the time taken until this point is calculated and presented in the figure. The next key task is calculated when the device receives the response and addresses it. Finally, the authentication process ends with the node verifying the response received from the device and deciding whether to provide access or not.

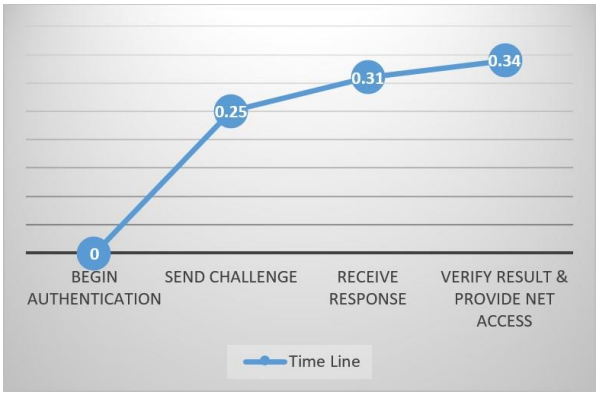

Fig. 6: Scenario 2 timeline

Similar to Scenario 1, the simulation for Scenario 2 is also conducted according to the process explained in Section 3.2. This simulation is conducted without the presence of the WR and uses the K_{CR} for encryption and decryption. Fig. 6 displays a timeline of the authentication process starting at 0 seconds and finishing at 0.34 seconds while mapping the key tasks in between.

The performance analysis for Scenario 1 and 2 based on resource consumption is also conducted. Fig. 7 displays the memory consumption for both Scenario 1 and 2. Fig. 8 shows the CPU utilisation.

As we can see in the above figures, the full authentication takes almost 3 seconds more than the quick authentication. However, the presence of both scenarios with their conditions together provides better security for the network. In terms of the performance analysis, both the scenarios have similar resource utilisation, which is mainly required for encryption and decryption purposes.

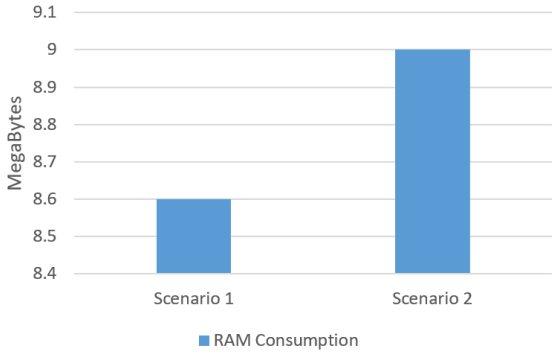

Fig. 7 Memory Consumption

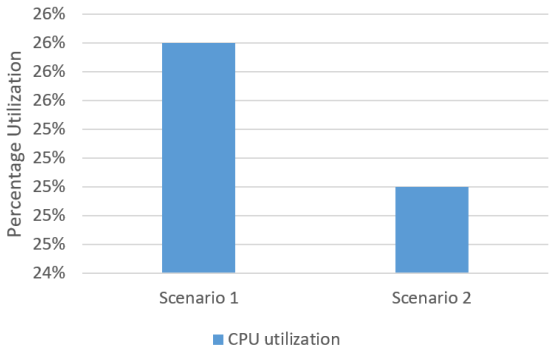

Fig. 8. CPU usage

6. Conclusion and Future Work

Dynamic wireless mesh network is an emerging technology in the area of self-sustained formation of networks and holds key to evolve into next generation communication network. However, it is limited only by the static protocols and rigid security frameworks, which are not suitable for the dynamic network.

The dynamic wireless mesh network requires new protocols and security models that are flexible and can adapt to various scenarios. The hybrid authentication scheme presented in this paper is one such aspect, which works according to the network rather than have the network work according to it.

Along with the flexibility, the security model also needs to use new methods to provide higher levels of security as mesh networks are prone to various attacks as discussed in Section 1. With more security schemes along with new dynamic protocols like GLOR, we hope, the dynamic wireless mesh network can become better managed, more secured and scalable for the future.

Our next challenge will be to incorporate the new hybrid authentication mechanism along with other security features of the GLOR security model and implement in a real-world scenario. The observations for further testing and implementation will also help in revealing more areas that require attention and will accordingly aid in the overall improvement of the GLOR security model.

7. References

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

[2] 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, pp. 891-898, 2016.

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

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

[5] P. Zimmermann. "A proposed standard format for RSA cryptosystems." IEEE Computer, Vol. 19, pp. 21-34, 1986.

[6] NIST FIPS. "197: Advanced Encryption Standard (AES)" Federal Information Processing Standards Publication 197, US Department of Commerce/NIST, November 26, 2001.

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

[8] T. Clausen, and P. Jacquet, "Optimized link state routing protocol (OLSR)", RFC 3626, <http://www.rfc-editor.org/info/rfc3626>, 2003.

[9] T. Clausen, C. Dearlove, and J. Dean, "Mobile ad hoc network (MANET) neighborhood discovery protocol (NHDP)", RFC 6130, <http://www.rfc-editor.org/info/rfc6130>,2011.

[10] T. Clausen, C. Dearlove, P. Jacquet, and U. Herberg, "The optimized link state routing protocol version 2", RFC 7181, <http://www.rfc-editor.org/info/rfc7181>,2014.

[11] C. Dearlove and T. Clausen, "An optimization for the mobile ad hoc network (MANET) neighborhood discovery protocol (NHDP)", RFC 7466, <http://www.rfc-editor.org/info/rfc7466>,2015.

[12] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc on-demand distance vector (AODV) routing", RFC 3561, < http://www.rfc-editor.org/info/rfc3561>, 2003

[13] J. Sen, "Security and privacy issues in wireless mesh networks: A survey ", Wireless networks and security. Springer Berlin Heidelberg, pp. 189-272, 2013.

[14] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler and D. Raffo, "Securing the OLSR protocol", 2nd IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2003), pp. 25–27, 2003.

[15] M.G. Zapata and N. Asokan, "Securing ad hoc routing protocols", 1st ACM Workshop on Wireless Security (WiSe 2002), pp. 1–10, 2002.

[16] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M. Belding-Royer, "A secure routing protocol for ad hoc networks", 10th IEEE International Conference on Network Protocols (ICNP 2002), pp. 78–87, 2002.

[17] P. Papadimitratos and Z.J. Haas, "Secure routing for mobile ad hoc networks." SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS 2002), pp. 27–31, 2002.

[18] Y.C. Hu, D.B. Johnson and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002), pp. 3–13, 2002.

[19] P. Papadimitratos and Z.J. Haas, "Secure data transmission in mobile ad hoc networks", ACM Workshop on Wireless Security (WiSe 2003), pp. 41–50, 2003.

[20] S. Yi, P. Naldurg and R. Kravets, "Security-aware ad hoc routing for wireless networks", ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001), pp. 299–302, 2001.

[21] P. Papadimitratos and Z.J. Hass, "Secure link state routing for mobile ad hoc networks", Symposium on Applications and the Internet Workshops (SAINT 203 Workshops), pp. 379–383, 2003.

[22] Y. Lee, H.K. Lee, G.Y. Lee, H.J. Kim and C.K. Jeong, "Design of hybrid authentication scheme and key distribution for mobile multi-hop relay in IEEE 802.16 j", 2009 Euro American Conference on Telematics and Information Systems: New Opportunities to increase Digital Citizenship, p. 12, 2009.

[23] A. Nanda, P. Nanda, X. He, A. Jamdagni and 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 (IEEE TrustCom-17), pp. 269-276, 2017.

[24] X. Li, J. Niu, S. Kumari, F. Wu, A. Sangaiah, and K-K R. Choo. "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments." Journal of Network and Computer Applications, 2017.

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

[26] F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K-K R. Choo, M. Wazid, and A. Das. "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment." Journal of Network and Computer Applications, Vol. 89, pp. 72-85, 2017.

[27] Y. Yang, Z. Wei, Y. Zhang, H. Lu, K-K R. Choo, and H. Cai. "V2X security: A case study of anonymous authentication." Pervasive and Mobile Computing, 2017.