 ISBN – 978-93-5407-803-3

COMMUNICADO – Messenger Using Adhoc Infrastructure

Kartik K[1], Hemant K[1], Jay Prakash P[1], Hari Om A[1]
[1]SJB Institute of Technology, Bangalore

Abstract: Authors believe that using dynamic adhoc network architecture can provide secure network communication at places where there is internet monitoring or no physical infrastructure. This paper deals with setting up of communication between devices in a wireless-adhoc environment. Here, Multiple client-side devices can communicate with multiple server-side nodes in an adhoc manner. Such a network would help in avoiding monitoring from Internet Service Providers, Government Entities, and prevent Man-in-the-middle attacks and provide an instant internet replacement for communication. Thus, communication can be established between multiple clients connected with the node. Emergency communication over radio channels can also be implemented in the future on the device by utilizing the LoRA module for long-range data transfer at a lower baud rate. This network is secure due to our use of state-of-the-art encryption protocols to provide end-to-end protection for every message.

Keywords: Wireless adhoc, Security, Raspberry-pi Zero W, Communication, Privacy.

Introduction

Amidst the increase in control over the Internet from Government agencies and large multi-million corporations, communication has become hugely dependent on applications provided by them or indirectly under their control. Such a level of control makes it hard to communicate information that is against them either as a journalist or to criticize them. This spying makes it almost impossible for citizens to form an awareness campaign or carry out peaceful protests which, in turn, hinders the right of freedom of speech and opinion.

Most of the major services can be monitored by these giants and those which cannot be monitored are dismissed, it makes communicating a dire task. When the entire internet is being monitored, there is no other option but to keep the communication off the internet by building a network, a network that is decentralized and under citizen's control.

This paper tries to provide a solution to such a situation by implementing a hardware-based dynamic ad-hoc network that will decentralize the communication and will be separate from the Internet. This network provides secured data transmission and has checks to maintain data integrity. Furthermore, this network's range increases by increasing the number of nodes.

Literature Survey

The main issues with existing systems are the security issues and the power consumption of devices that utilize wireless-adhoc on their devices directly. The constantly changing nature of the network topology coupled with data transmission in an open medium makes it highly susceptible to attacks and increases energy consumption due to its dynamic nature. Security issues concerning data confidentiality, availability of systems and applications, authentication, system integrity are just as threatening as in conventional networks. [1]

Vulnerabilities can lead to message eavesdropping, injection of fake messages, denial of service attack, or poor monitoring of routing information. MITM (Man-in-the-middle), Eavesdropping, Sybil Attack, Impersonation are some of the major attacks that can compromise such a network that is based purely on adhoc without using a node relay mechanism. [2, 6]

Challenges, Motivation and Objectives

No centralized administration entity is available to manage the operation of the different mobile nodes, so autonomous administration is required. Devices need to be able to connect and disconnect randomly and it should not affect the network, so implementation of dynamic topology is necessary [3]. Device discovery needs to be done to inform the connection of new users. Limited transmission range imposes a constraint on the usage and thus, it needs to be increased without too great a loss in quality of service. The device needs to run on limited resources and should be scalable to support more devices easily.

Motivation

Having all those implementations on user devices can be difficult as it increases the power consumption and causes the user's device to heat up while also decreasing its routing capability. Thus, adhoc devices need to be separated into nodes to facilitate all these without causing unnecessary strain on user devices.

Objectives
To separate the routing and network maintenance services from communication services for easy scalability.
This will make the end-user deal only with communication while the nodes separate from the user deal with the heavy lifting of maintaining the network.

Concrete objectives

- Creating a set of nodes via arm-based devices that will dynamically link with each other and an application that communicates on these nodes in a decentralized fashion to share data that can be encrypted.
- Protect network connectivity over multi-hop wireless channels.

Methodology
This project has two major bifurcations, one involving devices with arm-based architecture and other involving devices used to interact with them, such as smartphones.
For the hardware devices, raspberry pi zero will be used as nodes and will act as the endpoints for connecting devices such as smartphones which will be further mentioned as the client device.

The client device will have the front-end of the application which will encrypt the message with the PGP key and the encrypted message will be transmitted to the nearest node of the ad-hoc mesh. This node will act as the messenger node and then pass on the data with its encryption (AES-256) to its next node to pass on the information to the node which is nearest to the destination client. The end node will send the decrypted message to the destination client and the client's device will perform the last decryption using its PGP key to get the resulting message.

This is done by building this using small raspberry pi zero devices using custom ad-hoc routing algorithms which will be used to send the information to the nodes, for the client an application will be used to facilitate the communication.

Hardware Nodes
The software for routing is built with a Linux base built with Debian derived operating system and thus the source code will use a combination of C, C++, and Bash for the binary and the code will also use Python and Nodejs for the various library frameworks required for ad-hoc message transmission.
This device architecture will be replicated with all the other nodes and the resulting mesh network will from now on be referred to as the secured mesh. This secured mesh will only allow the nodes which have communicated its key and have been verified as a secure node. Each secured node will have a dynamic number of nodes determining on its latency of transmission.

Software Client
The software client will be handling the message transmission to other clients and the first of two-point encryption, which is GPG. The client when connected to the adhoc network will get the required IP from the node in which it is connected and after getting the IP the client will provide a socket address from the running service in the node. This running service will then associate the node in question with the established socket address in a HashMap and when another client requests to connect to this client it will be provided with a socket address and thus they can start communication between each other.
For the GPG, the client will have to register itself to provide and publish its key details to the keyserver. When a device needs to send a message to another client this message will be encrypted with the public address of the recipient and thus only the recipient will be able to decrypt the message with their private key.

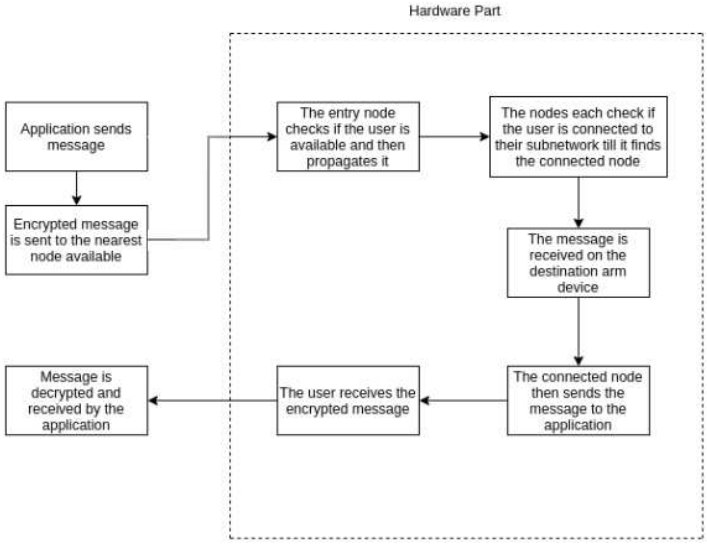
Flow and Functionality
First, a node is created with the predetermined subnet with pre-shared access key and the adhoc network is established, after the network is established and visible, this node will start the messaging service on one of its fixed ports after checking for free ports. This service will handle the connection handling between the client devices and provide the socket address of the client when it is requested. It does this by maintaining a record of all the connected devices in a HashMap and then returning the port of the client from the registered client list. The registered client list can be hard coded if it is a private network so no new clients other than the ones registered are served.
Multiple such nodes can be established by connecting to this barebone network which enables increases in range, this creates a network of hardware nodes waiting for clients to join and register their details.
The network infrastructure can be seen in Figure 1, here a client connects to the adhoc network and registers its details

with the node, providing its address. When another client joins the network and wants to communicate with this client, it requests for connection based on the client details and it will be provided the socket address and thus both the clients are connected with the help of the node.

The client-one will then send a message which is encrypted with a PGP key of the client-two user to the node which then encrypts if it's more than one hop away with AES and if it's less than one hop away then transmits it to client-two without AES encryption. The client-two will receive a message from the client-one which then decrypts with its PGP key to receive the message. In a more than one node network, when the message is sent to the entry node and the node checks for the location of the client (further referred as client-three) and determines that it is more than one hop away. It encrypts the data with AES and sends it to the nearest node (entry node). This node will forward the message until the node where the client-three is situated. The final node (destination node) will decrypt the AES message and forward the message to client-three who then proceeds to decrypt the PGP message.

This type of message will thus have end-to-end encryption and will be secure from a man-in-the-middle attack. Though the Quality of Service will decrease due to a bit of latency unless the message is very huge and the client a lot of hops away it would not be too bad.

This can be run on a small power bank as shown in Figure 2.



\

Figure 2. Raspberry pi zero node running on a power bank

Results and discussion

This network architecture can be used for places with active internet monitoring or areas within remote regions where communication is difficult or the cost to set up the network infrastructure is high.

This product can be coupled with other similar devices to extend the range of the network but adding more nodes would result in more latency and the Quality of Service (QoS) decreases significantly due to the security overhead as well as the transportation of the data to multiple nodes. Thus it is found that even with the decreased cost of the device and easy configuration it is not feasible to be used for a large number of users spread over a large distance unless it uses better wireless adapters with much farther range than available on the cheap ready to use devices. A NodeMCU can be utilized if a raspberry pi zero (Rpi zero) is not available and range needs to be increased urgently. This will lower the transmission speed, refer Figure 3, but it can be used at places when a suitable arm-based device is not available. Any wireless extender device can be utilized but the authors have considered NodeMCU as it is cheap and widely available and utilizes similar or lower power consumption to raspberry pi zero.

The network runs on very low current and can be used with a power bank, so it is very portable. Thus, energy consumption of the device is very minute and can be deployed as soon as required without any infrastructure delay.

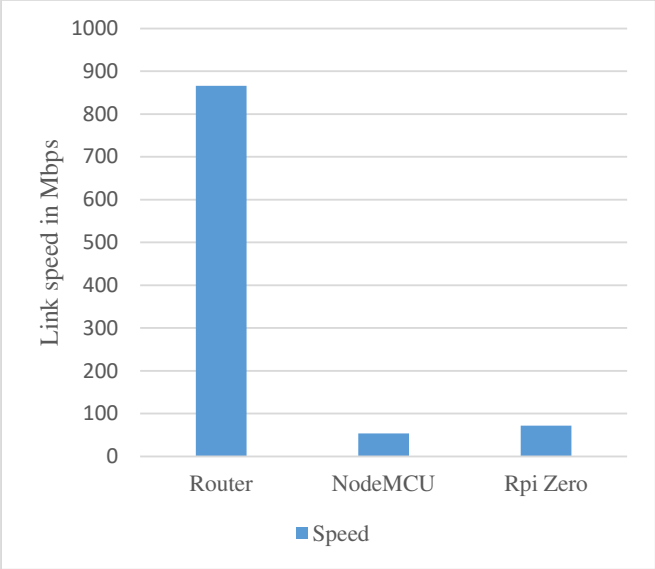


Figure 3. Comparison of network speed

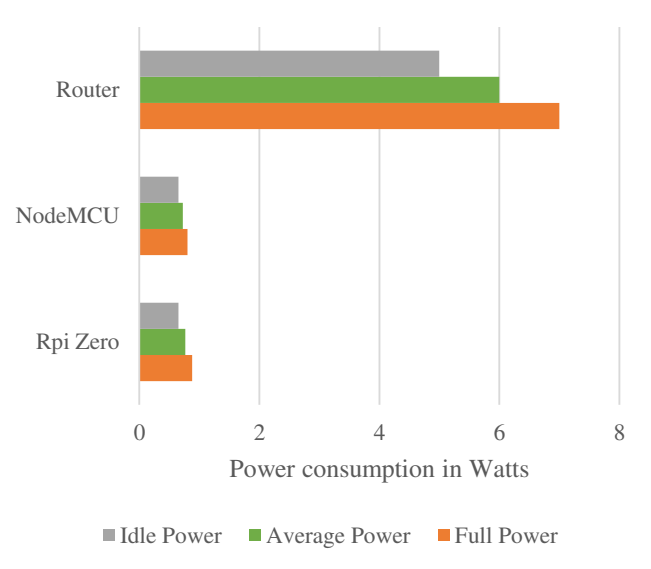


Figure 4. Comparison of power consumption

Table 1. Comparison of Power consumption and network speed

Comparison	Raspberry pi zero	NodeMCU	TP-Link (Gigabit Router)
Link Speed	72Mbps	54Mbps	866Mbps
Avg Power	0.765W	0.725W	6W

As Figure 4 suggests, these nodes consume almost 10 times less energy than a traditional router. Thus, it can safely be assumed that a small battery pack of 1000mAh will be sufficient to run a device for more than one day. This when coupled with its speed, refer Table 1, provides the portability to carry it around easily.

Conclusion

It is understood that its range and QoS are the main bottleneck for such a device and thus it is recommended to use this architecture at places where this would not have a drastic effect.

At a place where there is no network at all, it is much better to utilize a lower bandwidth device which is cheaper than no devices at all. This architecture can be improved much further with various new devices to make communication easier and secure at lower costs.

This architecture can be replicated on larger range devices instead of Wi-Fi which might be a bit more expensive but would provide such a large improvement in the range that it can be utilized for mountainous regions like parts of Uttarakhand, India (where it's very difficult to build a network tower due to landslides and cost). Here, devices that support LoRa (Long-range WAN) can be used and place it near possible areas for cheap and easy replacement.

References

[1] Security Issues with Mobile Ad-Hoc Networks. (2019, February 13). Retrieved from https://study.com/academy/lesson/security-issues-with-mobile-ad-hoc-networks.html.
[2] Reddy, K. R. K. (2018). Improved protocol design with security and QoS over MANET. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *3*(1), 735-739.
[3] Asma, A. (2013). Energy efficient routing algorithm for maximizing network lifetime of MANETs. *International Journal of Innovative Research in Computer and Communication Engineering*, *1*(8), 1683-1687.
[4] Sharma, M., Singh, M., Walia, K., & Kaur, K. (2019, October). Comprehensive Study of Routing Protocols in Adhoc Network: MANET. In *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (pp. 0792-0798). IEEE.
[5] Kock, B. A., & Schmidt, J. R. (2004, May). Dynamic mobile IP routers in ad hoc networks. In International Workshop on Wireless Ad-Hoc Networks, 2004. (pp. 130-134). IEEE.
[6] Arora, S., Nagrath, P., & Aneja, S. (2017, July). Secure encryption protocol for ad hoc networks. In *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.
[7] Stieglitz, S., Fuchß, C., & Lattemann, C. (2007). Mobile learning by using ad hoc messaging network.
[8] Othman, N. E., Hassan, R., & Hasan, S. S. (2014, December). The impact of mobility models on nodes cooperation in mobile ad hoc networks. In *2014 IEEE Student Conference on Research and Development* (pp. 1-5). IEEE.
[9] Zhang, T., Xu, C., Wu, M., Zhen, Y., Zhang, Q., & Wen, J. (2010, May). Implementation of Ad Hoc Network management system based on embedded ARM-Linux platform. In *2010 International Conference on Networking and Digital Society* (Vol. 1, pp. 167-170). IEEE.