SECURING FOG GATEWAYS WITH ASSURED QUALITY OF SERVICE

Geogen George*, Aditya Anil,
Department of Information Technology,
Faculty of Engineering and Technology,
SRM IST
geogen007@gmail.com,
2121fa04060@gmail.com

July 9, 2018

Abstract

Fog Computing is a horizontal architecture that distributes computing, storage, control and networking functions closer to users along the cloud-to-thing continuum. It is very critical for the fog gateway to efficiently manage and distribute the resources to the devices without compromising the Quality of Service and the Security of the system, as it is limited with small amount of computation, storage and memory resources. In a scenario where the Fog gateway holds limited resources and there are numerous devices connected to it, the fog gateway must be able to decide which packet must be processed first according to their priority & Queuing mechanisms. At the same time, the incoming packets will be encrypted with different algorithms, the gateway should be able to identify and decrypt it. If there is a malicious node sending malicious requests the gateway must detect those, all these will require processing resource. But, due to limited resources on the gateways end we must optimize the QoS without compromising on the security aspects. In the Project we like to study the strength and weakness of
existing protocols and how QoS is affected when secure packets reach Fog Gateways. With this info, we like to propose best Secure Cryptographic algorithms suited for Energy and compute constrained WSN and Fog Gateways without compromising QoS to a large extent.

**Keywords:** Quality of Service; Control Topology; Internet of Things; Fog Computing; Simulation; Wireless; Parallel and Distributed; Simulation; resource allocation; Cloud Computing; Edge Computing; Resource Management; Network Security

## 1 INTRODUCTION

In the recent years, Cloud computing has facilitated many opportunities for enterprises by providing their customers a wide range of computing services. Current “pay-as-you-go” Cloud computing model becomes a very efficient substitute to managing and owning private data centers for consumers facing batch processing and Web applications. Cloud computing eases the end users and their enterprises from the specifications of various details such as computation limitation, storage resources and network communication cost. However, these advantages become a nuisance for latency-sensitive applications, which need nodes in the surroundings to fulfill their delay requirements. As the devices of Internet of Things and techniques are getting involved in daily life, the present Cloud computing model cannot satisfy the requirements of location awareness, mobility support and low latency.

In the existing traditional gateways, it can only perform communication between networks, it doesn’t have any computation, storage and processing power. In order to overcome these Fog gateways were introduced, but services like security and Quality of Services are not optimized. Fog Computing is a horizontal architecture that distributes computing, storage, control and networking functions closer to users along the cloud-to-thing continuum. It is very critical for the fog gateway to efficiently manage and distribute the resources to the devices without compromising the Quality of Service and the Security of the system, as it is limited with small amount of computation,
Figure 1: Fog Layer

storage and memory resources.

2 BACKGROUND

A. What is Fog Computing?
A horizontal architecture that distributes computing, storage, control and networking functions closer to users along the cloud-to-thing continuum.

B. Advantages of Fog Computing
Security - There is less proximity between devices so the chances of eavesdropping are low.
Cognition It has the ability to learn and function according to the user requirements
Agility It supports rapid innovation and affordable scaling
Latency Applications which need millisecond reaction timings are supported i.e. time sensitive functions are addressed properly.
Efficiency Fog’s closer proximity to endpoints with limited storage, memory, and computing functions will increase overall system performance and efficiency.

Fog Gateways Fog Gateways are devices capable of enabling small computations, Storage and transient memory designations.

3 RELATED WORKS

To highlight the aim of this paper, we present the parallel and distributed computing [1] field and its key techniques that are introduced to accomplish and achieve goals in few time. The example in Figure 2 describes two cases of performing a program of passwords encryption on a set of 1000 passwords. In the first case this program is performed on a single machine and assume that it takes $T_d=240s$ per password, that means $T_t=240000s$ for accomplishing all the computing. But in the second case this program is performed on 10 machines which cooperate and distribute the data between them and work simultaneously. Of course this case will be achieved on time. This model is implemented on parallel and distributed virtual machine PVM that orchestrates and manages the distribution of data and tasks between the nodes. There are several inspiring proposed PVM machines [2,3,4,5,6] that used different technologies from the use the MCC mesh to the use of FPGAs. However, the scalability and efficiency of these PVMs depend on the quality of the used middleware. So, we need to take into account the ability of the middleware to manage the computing performance (Load balancing, fault tolerance, optimize the communication cost) in order to ensure HPC. The Middleware is the main components in the distributed systems that can manage a set of heterogeneous nodes. The Multi Agent System MAS is a promising technology for implementing such middleware. However, the micro-services implement the flexibility with the others technologies trends and the easy integration in cloud to improve HPC.

Another paper has proposed adaptive computing methods for IoT networking at the network edges to optimize and control traffic flows and network resources [7]. The fog computing challenges at the edge routers that include QoS issues, network
provisioning, and resource management. With the REAC (Regressive Admission Control) method, the adaptive edge router monitors the link performance to admit the flows to the network in a way which handles congestion and preserves good quality for prioritized users. The QoS scheduling capabilities utilize FWQ (Fuzzy Weighted Queueing) to control traffic flows according to the prevailing traffic level in a smooth and fast way in heterogeneous networks. The developed mechanisms are able to react faster to traffic changes and guarantee better quality for prioritized traffic and at the same time preserving fairness to other flows than the traditional control and scheduling methods without adaptive characteristics. The developed overall system reacts to changes in the network QoS by determining decision-making procedures on the possible flow rejection, marking, or allowed bandwidth weight assignment, thus bringing cognition to the network path. In future work, the adaptive traffic management methods need to be evaluated and the scalability tested in a large-scale environment for combining the different algorithms optimizing the performance of the IoT applications. Testing these features as SDN and NFV components would also be beneficial for the resource usage optimization.
In a paper [8] researches for an effective use of resources across the cloud data centers (CDCs) and the micro data centers (MDCs) that reside at the edge. There are a set of challenges that have been discussed like Workload variations, Application structure, High degree of user mobility, Effective utilization of edge resources, shared micro data centers, distributed user base, Collecting metrics under hardware heterogeneity, Lack of benchmarks.

The paper [9] proposes a scheme that provides an efficient distribution of the certificate revocation information. It is an up-to-date approach where all revoked certificates are sent immediately from the CAs to the cloud, then to the fog computing devices. Immediate updating of the revocation information ensures the security of the certificate validation process and eliminates the risk of accepting a revoked certificate. They also discuss some major open research challenges for enhancing security and privacy issues in IoT using fog Computing like:

- Secure & Efficient Protocols
- Authentication
- Attack Detection
- Location Verification
- Access Control

Another paper [10] discusses Message Oriented Middleware (MOM) is a key technology in financial market data delivery. In this context we study the Advanced Message Queuing Protocol (AMQP), an emerging open standard for MOM communication. We design a basic suite of benchmarks for AMQP’s Direct, Fan-out, and Topic Exchange types. We then evaluate these benchmarks with Apache Quid, an open source implementation of AMQP. In order to observe how AMQP performs in a real-life scenario, we also perform evaluations with a simulated stock exchange application. All our evaluations are performed over InfiniBand as well as 1 Gigabit Ethernet networks.

ISO (International Organization for Standardization) proposed the OSI (Open System Interconnection) model, which was
primarily designed to enable multi-supplier computers to interact and communicate. The layered OSI architecture offers a general framework for building modular structures. It divides the network functionalities, that are involved in provisioning end-to-end data transmission, into hierarchical layers containing sub-tasks (sub-functions). OSI defines seven layers with hierarchy that goes from bodily to utility layers. These days, OSI is still a reference model, regularly used to explain and outline the distinctive tiers of networking protocols and their relationships with each other [11].

Some other important layered structure is the current internet architecture, which relies at the IP-based protocol stack. The focus in this architecture is the IP protocol. In order to introduce numerous functions and adapt it to unique and new services offered by the internet, the IP protocol can be mixed with several control protocols. UDP (User Datagram Protocol, protocol with mild requirements), TCP (Transport Control Protocol, protocol for dependable point-to-point data transport) and SCTP (Session Control Transport Protocol, protocol for dependable transport of message-oriented programs with support for multi-streaming and multi-homing). Lately, RTP (Real-Time Transport Protocol) is designed to work over UDP and support real-time programs. IP can be also enhanced with a purpose to meet the QoS requirements introducing Diff-Serv(Differentiated services) and Int-Serv(Integrated Services) QoS capabilities [12].

Yanchao Zhang et al. [13] have proposed a credit-based Secure Incentive Protocol (SIP) to stimulate cooperation in packet forwarding for infrastructure less MANETs. Liu et al. [14] have proposed the 2ACK scheme that has served as an add-on technique for routing schemes to detect routing misbehavior and to mitigate the adverse effect.

Syed Rehan Afzal et al. [15] have explored that the security problems and attacks in existing routing protocols and then they have presented the design and analysis of a secure on-demand routing protocol, called RSRP which confiscated the problems mentioned in the existing protocols.

Muhammad Mahmudul Islam et al. [16] have presented a possible framework of a link level security protocol (LLSP) to be deployed in a Suburban Ad-hoc Network (SAHN). They have analyzed various security aspects of LLSP to validate its
effectiveness. To determine LLSP’s practicability, they have estimated the timing requirement for each authentication process.

Shiqun Li et al. [17] have explored that the security issues of wireless sensor networks, and in particular propose an efficient link layer security scheme. To minimize computation and communication overheads of the scheme, they have designed a lightweight CBC-X Mode Encryption/Decryption algorithm that attained encryption/decryption and authentication all in one.

Stefan Schmidt et al. [18] have proposed security architecture for self-organizing mobile wireless sensor networks that prevented many attacks these networks are exposed to. In addition, it has limited the security impact of some attacks that cannot be prevented.

4 PROBLEM STATEMENT

The world is experiencing a huge rise of digitally generated information from Smart Things and Connected devices. Parallely, with the increase of Smart-phones & Apps enabling more end users to access data, computation power, control and manage their end devices in real-time. The usual cloud structures allow the smallest data to be passed through the central cloud via the edge node devices for computation, calculation and analysis which ultimately increases the latency. Fog Computing, enables the edge node devices to perform some local data processing, cache data management, dense geographical distribution, local resource pooling, load balancing, local device management, latency reduction for better QoS (Quality of Service) and edge node analytics resulting in better overall customer experience.

The idea of “fog computing” has been put forward as a bridge between the IoT devices and remote data centers. Some IoT devices can produce numerous huge data that need to be handled. By using fog computing, some amount of that processing operations can be pushed to the computing resources at the edge, by filtering and summarizing the information to reduce volume and enhance value and relevance.

Moving the intelligent process of information to the edge solely raises the stakes for maintaining the provision of those sensible
gateways and their communication path to the cloud. Once the IoT provides strategies that permit individuals to manage their daily lives, from locking their homes to checking their schedules to cooking their meals, entry period of time in the fog computing becomes a critical issue. Additionally, all the resilience and failover solutions that safeguard those processes can become even more crucial.

The gateways must strengthen the IoT architecture by taking in the brunt of processing work before pushing it to the cloud or the data center. Fog computing might fulfill the requirements for a very reliable low latency response by handling near the edge and process with heavy traffic volumes by using smart filtration and selective transmission. By this way, the smart edge devices can either handle or push the millions of work incoming from the sensors and surveillance monitors of the IoT, and transmitting only basic summaries and exception data to the cloud. By possessing complete and secure control over the edge gateways even when the networks are down and having the ground to maintain, provision and repair critical infrastructure will be important in maintaining the services affecting the daily lives of customers, who eventually become increasingly dependent on IoT functionality and to the complexities going on behind the scenes.

Resource constraint Fog gateways need efficient management of QoS and Security. In a scenario where the Fog gateway holds limited resources and there are numerous devices connected to it, the fog gateway must be able to decide which packet must be processed first according to their priority & Queuing mechanisms.

At the same time, the incoming packets will be encrypted with different algorithms, the gateway should be able to identify and decrypt it. If there is a malicious node sending malicious requests the gateway must detect those, all these will require processing resource. But, due to limited resources on the gateway’s end we must optimize the QoS without compromising on the security aspects.

In the Project we like to study the strength and weakness of existing protocols and how QoS is affected when secure packets reach Fog Gateways. With this info, we like to propose best Secure Cryptographic algorithms suited for Energy and compute constrained WSN and Fog Gateways without compromising QoS.
to a large extend. According to our initial study (Literature Survey), modifications of Cross Layer QoS parameters or developing a middle layer to handle Security will be best.

5 PROPOSED SOLUTION

The Advanced Message Queuing Protocol (AMQP) is also a middleware messaging standard set. It can be applied using either publish/subscribe or point-to-point communication patterns. AMQP has a layered architecture and is organized into different parts to reflect that architecture. AMQP [19] is an open standard application layer protocol for the IoT focusing on message-oriented environments. It supports reliable communication via message delivery guarantee primitives including at-most-once, at-least-once and exactly once delivery. AMQP requires a reliable transport protocol like TCP to exchange messages. By defining a wire-level protocol, AMQP implementations are able to interoperate with each other. Communications are handled by two main components as depicted in Fig. 3: exchanges and message queues. Exchanges are used to route the messages to appropriate queues. Routing between exchanges and message queues is based on some pre-defined rules and conditions. Messages can be stored in message queues and then be sent to receivers. Beyond this type of point-to-point communication, AMQP also supports the publish/subscribe communications model.

AMQP defines a layer of messaging on top of its transport layer. Messaging capabilities are handled in this layer. AMQP defines two types of messages: bare massages that are supplied by the sender and annotated messages that are seen at the receiver. In Fig. 4 the message format of AMQP is shown [11]. The header in this format conveys the delivery parameters including durability, priority, time to live, first acquirer, and delivery count.

The transport layer provides the required extension points for the messaging layer. In this layer, communications are frame-oriented. The structure of AMQP frames is illustrated in Fig. 5 [19]. The first four bytes show the frame size. DOFF (Data Offset) gives the position of the body inside the frame. The Type
Figure 3: Publish/subscribe mechanism of AMQP

Figure 4: AMQP Message Format
field indicates the format and purpose of the frame. For example, 0x00 is used to show that the frame is an AMQP frame or type code 0x01 represents a SASL frame.

![AMQP Frame Format](image)

Figure 5: AMQP Frame Format

With this info we like to propose best Cryptographic algorithms suited for energy and computation constrained WSN and Fog Gateways without compromising QoS to a large extent. According to initial studies modifications of Cross Layer QoS parameters or developing a middle layer to handle Security will be the best. Some of the QoS parameters that can be altered are:

- **Throughput**: Throughput is a connection-mode QOS parameter that has end-to-end significance. The throughput specification defines the target and minimum acceptable values for a connection.
- **Transit Delay**: The amount of time required to push all the packet’s bits into the Channel
- **Priority**: Highly sensitive packets are given priority bit and will be processed immediately.
- **Protection**: Using Lightweight Encryption techniques like H-MAC.

The AMQP Broker will be having an Exchange i.e. the communication between the nodes and then it is bonded to the
Queues. The Queuing mechanisms and the sizes can be altered for better throughput. The Routing metrics and the Priority bits can be added to the packets so as to reduce the transit Delay, these alterations can bring in better QoS in the Fog Gateways. In order to ensure security, we introduce H-MAC with SHA-1 encryption in the gateway which will ensure secure communication among the nodes.

6 MODULES

A. An AMQP Broker and enabling communication between Client and Server

Tmote Sky Tmote[20] sky platform is the wireless sensor module that has 1 MB external flash memory with two light sensors. Various applications can function on this platform, when programmed accordingly. The system contains integrated sensors, a radio chip and a micro controller, with the ability to go in sleep mode, thereby minimizing power consumption. The radio chip supports strong signals and data transfer at high speed. The Tmote sky platforms are gaining wide popularity in various fields like medical, commercial, domestic and industrial. Tmote sky facilitates secured network sharing and is convenient to install at home or in offices.

- Creating a Gateway with AMQP firmware in it.
- Creating a Client to communicate with the Broker
- Enabling 6LoWPAN communication among them
- Simulation of motes using Cooja[21]

6LoWPAN is a contorted acronym that combines the latest version of the Internet Protocol (IPv6) and Low-power Wireless Personal Area Networks (LoWPAN). 6LoWPAN [22], therefore, allows for the smallest devices with limited processing ability to transmit information wirelessly using an Internet Protocol.

Gateway: The gateway will act as an AMQP Broker, it will contain Queues and exchanges in it. All the messages between the clients will pass through the gateway. Client: There will be
AMQP Clients which will communicate with the Gateway and acknowledgements will be passed on.

B. Appending H-MAC Encryption and altering the QoS parameters in the broker firmware

The AMQP [23] Broker will be having an Exchange i.e. the communication between the nodes and then it is bonded to the Queues. The Queuing mechanisms and the sizes can be altered for better throughput. The Routing metrics and the Priority bits can be added to the packets so as to reduce the Transit Delay, these alterations can bring in better QoS in the Fog Gateways. In order to ensure security, we introduce H-MAC with SHA-1 encryption in the gateway which will ensure secure communication among the nodes.

- Adding H-MAC with SHA-1 encryption to the Firmware
- Setting up Priority bits in sensitive packets
- Altering the queues and routing metrics for better QoS
- Drawing out the graphs and simulation results
- Analyzing the results in all the scenarios

7 RESULTS AND OBSERVATIONS

The results clearly indicate that the motes are able to communicate via the AMQP broker and with modifications to the queuing mechanisms, we were able to achieve better results. When a packet reaches the gateway it goes through the exchange and then is routed to one of the queues. By enabling alteration to the routing metrics we could achieve optimized transit delay in the communication channel, the first bit of data unit passes the first given point and the moment that bit passes the second given point, plus the transmission time of the data unit comprises of the transit delay.

There was a significant increase in the throughput of the network i.e. the amount of data that can be sent and received
Figure 6: AMQP Broker Communications

Figure 7: Throughput performance graph
from one place to another in a given time period, typically measured in bits per second (bps).

The motes connected to the AMQP broker are using SHA-1 hashing to transmit messages in the network. By using SHA-1 we could ensure secure transmission of messages in the fog network.

Figure 8: Transit Delay in Network

Figure 9: CPU Utilization

Overall, we could optimize the QoS with limited resources on the gateway end by also keeping the security aspects intact. The secure
packets were transmitted with better Quality of service within a constrained and distributed environment.

8 CONCLUSION AND FUTURE WORKS

By using better optimized techniques for secure transmission of messages and resource allocation we can conclude that this is best suited for energy, compute and resource constrained wireless sensor networks or fog gateways without compromising quality of services to a large extent. The future works can include analysis against various fog layer attacks and providing a fully secure encrypted channel for communication. Providing mobility support is very essential for the clients. Intrusion Detection Systems can be Enabled. These mechanisms can be deployed in a resource constraint environment and can work in an optimized manner.

References


