

# Effective Implementation of IoT for Enhancing Cargo Container Security

Anagha Shinde

Assistant Professor, Vishwakarma Maritime Institute (VMI), Pune, India

**Abstract:** This paper discusses effective implementation of IoT to enhance container security in marine cargo industry. It is estimated that 90% of goods traded globally are moved by around 17 million containers. However it is very difficult to control and monitor the container contents. There are various challenges like spoilage, tampering, theft, smuggling of contraband materials even nuclear weapons. This calls for constant monitoring, analysis and reporting of various parameters like temperature, humidity, radiation inside containers throughout the journey. This is a complex problem as the paths of ships are often out of reach of conventional communication technologies and are subject to rough weather. Additionally metal containers limit range of RF signals. Various technologies like Satellite/RF/GSM Communication, Cloud Computing, Device Engineering, Last mile connectivity will be utilized for the purpose. This paper reflects our thought process on effective implementation of IoT techniques to enhance the end-to-end traceability and security of containers.

**Keywords:** Internet of Things (IOT), RF Signal, Cargo Security, Supply Chain Management.

## I. INTRODUCTION

Container Shipping is very popular and economical -In an average year, a large container ship travels three-quarters of the distance to the moon. That means in its lifetime it travels to the moon and back nearly ten times. A container of refrigerators can be moved from a factory in Malaysia to Los Angeles -- a journey of roughly 9,000 miles or 14,484 kilometers -- in just 16 days. The cost to transport a bicycle from Thailand to the UK in a container is about US\$10. The typical cost for shipping a DVD/CD player from Asia to Europe or the U.S. is roughly US\$1.50; a kilogram of. Coffee just fifteen cents and a can of beer - a penny. Large container ships can be operated by teams of just thirteen people utilizing sophisticated computer systems. Shipping is most carbon efficient means of transportation.

Cargo security is closely associated with an aggressive management position that all participants in the transportation transaction will act as one in combating the theft of goods. Cargo security activities may be broken into three distinct periods of time: prior to shipment, during shipment and after shipment. The majority of theft involving ocean shipment of cargo takes place at either the port of embarkation or the port of destination.



Fig 1: Cargo Carrying Container

The most important aspect to assess prior to shipment is how well you know your trade intermediaries. Ensuring the security of all the information related to your cargo is imperative. The first step is to make certain that you check the references of any trade intermediary used to assist your import/export activities. Trade intermediaries have knowledge of shipping routes, types of goods being shipped, cargo value and other sensitive shipping information that could aid thieves. Even if you deal with honest and reputable intermediaries, you should evaluate what information security system they use for their own records and which people have access to transaction records. The security of the offices of any firm or person assisting you with import/export transactions should also be checked to reduce the risk of break-ins and other thefts. Improper security at the point-of-origin terminal can sabotage a transaction as well.

Terminals are normally owned by others (e.g., a government), however, questions related to security must be posed by both the cargo owner and the shipping company. History has shown that many ships are targeted because their cargo was observed while it was being loaded or when it was being packed into containers. All pre-shipment warehousing, packing and transportation must be reviewed for security concerns to ensure that unfriendly eyes are not scouting your shipment. Again during Shipment, once cargo is placed on board a vessel, many owners feel their worries are almost over. That is far from correct. Without proper security, a voyage of several weeks may allow ample shopping time for those bent on criminal activity. After Shipment, the main concern after the voyage is complete is terminal security. This is also one of the major areas of concern related to homeland security and terrorism. It is common for security in developing nations to be less stringent than in industrialized countries, so they tend to pose an inherently greater risk. All of the questions associated with the

point-of-origin of cargo also apply to the destination port.

While sailing number of containers are being transmitted from source to destination. Through this container all types' goods are transmitted from one area to another. While transimition between transmitters to receiver, there are chances of damaging of goods contain inside all containers. For some goods it is necessary to maintain proper temperature to keep it fresh through all voyage from source to destination. In short all this communication requires proper maintenance of goods inside the containers. So numbers of wireless sensor are fitted inside all containers. Sensors these sensors are Temperature, Pressure, Flow, Level, Humidity etc. These sensors detect exact condition of goods being transmitted inside the container. Sensors detect condition of goods and converts that data into another usable form for example electrical form which information further transmitted for controlling purpose.

There are 90% of worlds trade happens through shipping .95% of Americas import and export happens through shipping. There are @ 17 million containers in world. There are almost 6000 linear ships working on 400 linear services providing weekly departures. US and China are 2 largest users on container shipping worldwide DHS has delayed until 2016 the implementation of key sections of the SAFE Port Act of 2006, which requires that 100 percent of U.S.-bound ocean containers be scanned at the foreign port of origin. - Has been doing same every 2 years!!!"However due to recent intelligent reports suggesting that terrorist may use shipping containers to bring nuclear weapons on US soil DHS is looking for more practical approach to ensure 100% port safety without affecting trade.

## II. PROPOSED WORK FOR CARGO SECURITY

For Cargo Security RF transmitter with multiple sensors to be fitted inside container. [3]

- 1) Sensors can be temperature, light, humidity, radiation etc. and will be modular in nature so can be added/removed to RF unit during installation based on client need.
- 2) RF transreciever device outside container door
- 3) RF network will operate in mesh topology to avoid blind spots and line of sight limitations.
- 4) Control desk will have RF to VSAT convertor, data then uploaded on VSAT/Geo Stat / LEO satellite.[1]
- 5) There will be provision to upload data to GSM network which will enable tracking containers during road shipment and when they are in dock at lower cost.
- 6) On shore data center will be equipped with VSAT antenna / Satellite gateway which then feeds data on cloud.
- 7) Cloud hosts various monitoring and tracking applications along with inventory database and supply chain management system.[2]
- 8) User can access data through web portal

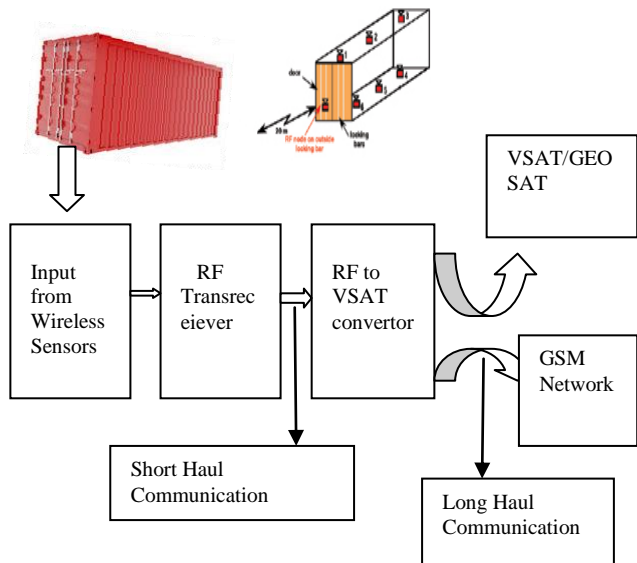


Fig 2: Effective Implementation of IOT for Cargo Security

## III WIRELESS SENSORS

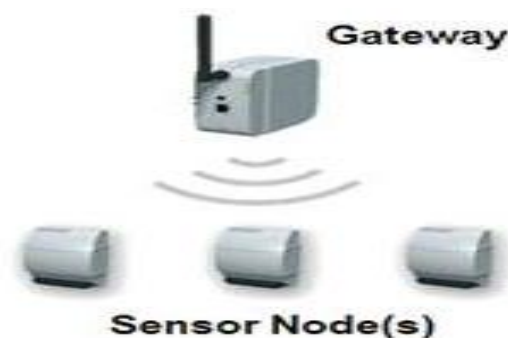


Fig3: Wireless Sensors

Sensors are sophisticated devices that are frequently used to detect and respond to electrical or optical signals. A Sensor [12][13] converts the physical parameter (for example: temperature, blood pressure, humidity, speed, etc.) into a signal which can be measured electrically. To explain this considers the example of temperature. The mercury in the glass thermometer expands and contracts the liquid to convert the measured temperature which can be read by a viewer on the calibrated glass tube.

There are certain features which have to be considered when we choose a sensor. They are as given below:

1. Accuracy
2. Environmental condition - usually has limits for temperature/ humidity
3. Range - Measurement limit of sensor
4. Calibration - Essential for most of the measuring devices as the readings changes with time
5. Resolution - Smallest increment detected by the sensor
6. Cost
7. Repeatability - The reading that varies is repeatedly measured under the same environment

Classification based on property is as given below:

- Temperature - Thermistors, thermocouples, RTD's, IC and many more.
- Pressure Sensors - Fibre optic, vacuum, elastic liquid based manometers, LVDT, electronic.
- Flow - Electromagnetic, differential pressure, positional displacement, thermal mass, etc.
- Level Sensors - Differential pressure, ultrasonic radio frequency, radar, thermal displacement, etc.
- Proximity and displacement - LVDT, photoelectric, capacitive, magnetic, ultrasonic.

#### IV. RF TRANSMITTER WITH MULTIPLE SENSORS

In this approach RF transmitter with multiple sensors to be fitted inside container.

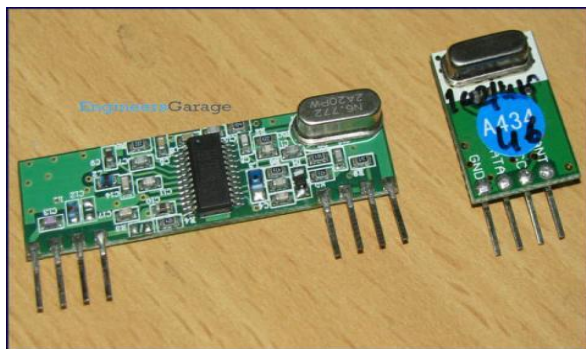


Fig 4: RF Module

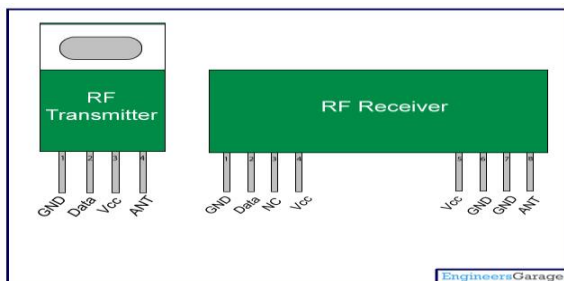


Fig 5: RF Transmitter with Receiver

The RF module, as the name suggests, operates at Radio Frequency. The corresponding frequency range varies between 30 kHz & 300 GHz. In this RF system, the digital data is represented as variations in the amplitude of carrier wave. This kind of modulation is known as Amplitude Shift Keying (ASK) [4].

Transmission through RF [5] is better than IR (infrared) because of many reasons. Firstly, signals through RF can travel through larger distances making it suitable for long range applications. Also, while IR mostly operates in line-of-sight mode, RF signals can travel even when there is an obstruction between transmitter & receiver. Next, RF transmission is more strong and reliable than IR transmission. RF communication uses a specific frequency unlike IR signals which are affected by other IR emitting sources.

This RF module comprises of an RF Transmitter and an RF Receiver. The transmitter/receiver (Tx/Rx) pair operates at a frequency of 434 MHz. An RF transmitter receives serial data and transmits it wirelessly through RF

through its antenna connected at pin4. The transmission occurs at the rate of 1Kbps - 10Kbps. The transmitted data is received by an RF receiver operating at the same frequency as that of the transmitter.

The RF module is often used along with a pair of encoder/decoder. The encoder is used for encoding parallel data for transmission feed while reception is decoded by a decoder.



Fig 6: RF Network

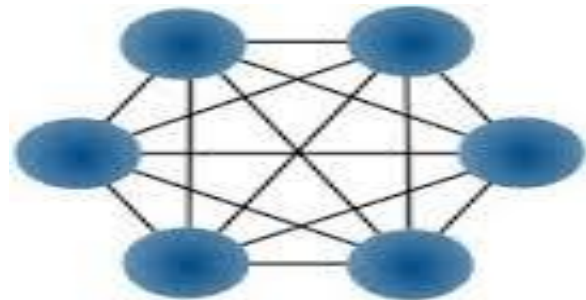


Fig 7: RF Communication with Mesh Network

Mesh network topology is a key network architecture in which devices are connected with many redundant interconnections between network nodes. If any batteries or nodes fail in a wireless mesh topology, many other ways are available for two nodes to communicate. A mesh topology is often used in conjunction with other topologies – such as Star, Ring, and Bus – to form a hybrid topology. Some WAN architecture, such as the Internet, employs mesh routing. This allows the Internet sites to communicate even during a war. The two types of mesh topologies are full mesh and partial mesh. Full mesh topology occurs when every node has a circuit connecting it to every other node in a network. Full mesh yields the greatest amount of redundancy, so if a node fails, network traffic can be directed to any of the other nodes. Full mesh is usually reserved for backbone networks. With partial mesh, some nodes are organized in a full-mesh scheme, but others are connected to only one or two in the network. Partial mesh topology is commonly found in peripheral networks connected to a full meshed backbone. Partial mesh is less expensive to implement but yields less redundancy than full mesh topology.



RF Transceiver is basically a frequency converter. It consists of two parts frequency up converter and frequency down converter. Up converter converts modulator frequency usually in either 70/140 MHz to satellite frequency bands as per satellite in use for particular location/application. Down converter does reverse of the up converter. In addition to frequency conversion both provide gain to the signal as per VSAT link budget and the same need to be adjusted as per need of the link using attenuation settings available in RF transceiver in both up/down link. Refer following links for RF transceiver basics and for Rf transceiver design and development.

**RF power amplifier:** RF Power amplifier is the unit which provide power amplification without any frequency change before signal is transmitted to the antenna and consecutively to the air. Refer following link to know more on RF Power Amplifier basics, various stages, classes, specifications and design of RF amplifier with example.

**RF LNA** is the low noise amplifier used in VSAT. As the signal is received by antenna is composed of noise as well as useful information signal part. In addition it is very low in the power level. LNA's job is to boost this low level of signal to the sufficient level considering less amplification of noise part, so that adequate C/N is maintained. For more on LNA and LNB refer following links. [5][6].

Satellite modem provides two major functionalities in the VSAT. The first one is it makes link reliable by adding forward error correction functionality using various techniques such as convolution coding/turbo coding and so on. The second one is that it does task of modulation and demodulation. There is various modulation techniques used in modem, the most popular among them are QPSK/8PSK. To know what modulation is, various modulation techniques and satellite modem design refer following links.

Antenna is basically a electro-magnetic frequency transducer. It sends and receives EM waves of various frequency bands. Antenna diameter and aperture vary band to band. Hence C band antenna design is different than Ku band. The signal to be transmitted will be provided to antenna by Power Amplifier. The signal received by Antenna is fed to LNA.

VSAT network architecture is the way Hub station and/or VSATs are interfaced with satellite to provide the service. There are five main topologies exist, viz. broadcast, point to point, point to multipoint (star), mesh, hybrid. Let us understand each of this VSAT topology.

In Broadcast type, there is a single broadcasting station interfaced with satellite and satellite will relay signals to all the VSATs. Here broadcasting station-satellite-all VSATs link exist.

In point to point type of topology, two VSATs communicate via satellite using dedicated assigned channel. So here VSAT1-Satellite-SAT2 dedicated link exist.

In Star topology, there are three entities hub station (usually with larger antenna), VSATs and Satellite. All the communications between VSATs happen through Hub

station. Hence here if VSAT1 and VSAT2 need to communicate then, link is VSAT1-satellite-Hub-Satellite-VSAT2. Hence two hop communication is needed to communicate between any two VSATs in the network.

In Mesh type of topology, VSATs can communicate with one another directly and no Hub station is needed. But each VSAT need to be complex owing to more functionality required similar to the Hub station. Also antenna specifications need to be different than star type of topology. In Hybrid type is the combination of both star and mesh type. Here few of the VSATs communicate via Hub and few can communicate directly with one another

## V. RELATED WORK

In the last few years, the Topic-based on Cargo Security have been proposed. keep on propose the technology with Infrared ID with multiple sensors. But there are limitations as proposed technology is limited to specific area. It does not suit for long distance communication.

## VI. CONCLUSION

The proposed method RF transmitter with multiple sensors to be fitted inside container. Sensors can be temperature, light, humidity, radiation etc. and will be modular in nature so can be added/removed to RF unit during installation based on client need. RF Transreceiving device outside container door. RF network will operate in mesh topology to avoid blind spots and line of sight limitations. Control desk will have RF to VSAT convertor, data then uploaded on VSAT/Geo Stat / LEO satellite. Advantage of further method is for security of cargo container .Along with security there is a provision of controlling of goods carried out inside container. Proposed method is useful for longer distance communication. It has provision of tracking of transportation which is helpful for supply chain management.

## REFERENCES

- [1] R. Want, RFID explained : a primer on radio frequency identification technologies, Synthesis Lectures on Mobile and Pervasive Computing Vol. 1, No. 1, pp. 1–83, 2006
- [2] L. Overmeyer, S. Vogeler, RFID: Grundlagen und Potenziale, Logistics Journal, Vol. 5, pp. 1–12, 2005
- [3] D. Hahnel, W. Burgard, D. Fox, K. Fishkin, M. Philipose, Mapping and localization with RFID technology, in IEEE International Conference on Robotics and Automation, Vol. 1, No. 1, pp. 1015–1020, 2004.
- [4] P. Wilson, D. Prashanth, H. Aghajan, Utilizing RFID signaling scheme for localization of stationary objects and speed estimation
- [5] R. Miesen, F. Kirsch, M. Vossiek, Holographic localization of passive UHF RFID transponders, in IEEE International Conference on RFID, pp. 32–37, 2011.
- [6] M. Fujimoto, N. Uchitomi, A. Inada, T. Wada, K. Mutsuura, H. Okada, A novel method for position estimation of passive RFID tags; Swift Communication Range Recognition (S-CRR) method, in Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, pp. 1–6, 2010..
- [7] Y. Park, J.W. Lee, S. Kim, Improving position estimation on RFID tag floor localization using RFID reader transmission power control, in IEEE International Conference on Robotics and Biomimetics, pp. 1716–1721, 2009.14.
- [8] T. Hori, T. Wda, Y. Ota, N. Uchitomi, K. Mutsuura, H. Okada, A multi-sensing-range method for position estimation of passive RFID tags, in Networking and Communications, 2008. WIMOB

- '08.IEEE International Conference on Wireless and Mobile Computing, pp. 208–213, 2008.
- [9] Bing, K. Fishkin, S. Roy, M. Philipose, Unobtrusive long-range detection of passive RFID tag motion, in IEEE Transactions on Instrumentation and Measurement, Vol. 55, pp. 187–196, 2006.9 of mobile objects, in IEEE International Conference on RFID, pp. 94–99, 2007..
- [10] A. Bouzakis, L. Overmeyer, RFID tag positioning with the aid of an active electronically-steered array, in IEEE International Symposium on Personal, Indoor and Mobile Radio Communications PIMRC12, pp. 2483–2488, 2012
- [11] Ryan Newton and Matt Welsh. Region streams: Functional macroprogramming for sensor networks. In Proceedings of the First International Workshop on Data Management for Sensor Networks (DMSN), Toronto, Canada, August 2004.
- [12] Adrian Perrig, John Stankovic, and David Wagner. Security in wireless sensor networks. Commun. ACM special issue: Wireless sensor networks, 47(6):53–57, 2004..
- [13] Jan Steffan, Ludger Fiege, Mariano Cilia, and Alejandro Buchmann. Scoping in wireless sensor networks: A position paper. In Proceedings of the 2nd Workshop on Middleware for Pervasive and Ad-hoc Computing, pages 167–171. ACM Press, October 2004.
- [14] Ronald Watro, Derrick Kong, Sue fen Cuti, Charles Gardiner, Charles Lynn, and Peter Kruus. TinyPk: securing sensor networks with public key technology. In SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pages 59–64, New York, NY, USA, 2004. ACM Press.