Dual Synchronization Algorithm for Internet of Things Communication Security

Venkatesha S
E&C Department, 7th Semister BNMIT,
Banashankari Bangalore, India

***Abstract*—This paper aims to incorporate Dual Synchronization security algorithm in Internet Of Things (IOT) to control smart home appliances using Bluetooth connectivity and android phone. The IOT incorporate Bluetooth enabled smart phone to connect with Bluetooth master module which drives the connected appliances. This IoT infrastructure adopts dual synchronization algorithm to eliminate any Cyber\Embedded security risks involved within communication networks.**

Keywords—Bluetooth,Embedded,security, Bluetooth connectivity, android, Secured IoT.

I. INTRODUCTION TO IOT

The Internet of Things (IoT) is a framework and infrastructure created between remote objects which are connected and controlled using internet media, the connection and communication can be

Infrastructure to Infrastructure objects
Infrastructure to moving objects like vehicle
Vehicle to vehicle (Intra vehicle and Inter vehicle)The

IOT has 2 major parts
The cloud\Web side
The Embedded side

The cloud side connectivity establishes internet based infrastructure for longer distance connectivity for monitoring and controlling the devices, whereas the embedded\physical objects side implements the electronic\electrical hardware components along with built-in intelligent algorithms to perform the specific activity based on the supervisory commands either from remote devices or connected internal devices.

The Whole system becomes a complex structure (Fig1 and Fig2) of infrastructure, electronics hardware, software, sensors, actuators, and network connectivity (either wired or wireless media – telecom services) enabling objects to excha nge the information.

This global infrastructure connects multiple logical devices present at different geographic location to perform specified activity either monitoring or controlling from remote distance by exchanging information over internet and Wi-Fi connectivity. This advanced infrastructure framework will enable less physical systems.

The connectivity is majorly by Internet for cloud side, where as the embedded connectivity can be by any wireless media. communication media requirements, which help society in lesser nfrastructure over heads and more efficient Bluetooth wireless communication is used for the demonstration.

Fig1 IO_T

Fig2 IOT

II. THE CHALLENGES

The cyber security and embedded security is becoming a critical challenge in modern world, where most of the populous security algorithms are becoming obsolete. This challenge is throwing lot of innovation openings in the cyber security space.

The organizations across the world are already moving ahead with the On The Air (OTA) programming for embedded devices using boot code modules, to make the embedded product more configurable to perform multiple operations as against earlier days of implementation where the device performs specific operations. This concept is also throwing a bigger challenge for more robust cyber security implementation.

III. THE IDEA

This paper explains and demonstrates a basic dual synchronization security algorithm to secure from cyber\embedded hacking.

The Dual synchronization algorithm performs 2 levels of handshaking before the device performs any operation for a specific command.

1. A synchronization counter will be implemented in Transmitter and Receiver devices.
2. Both the transmitter and receiver devices will be incrementing the synchronization counter on every communication transaction (Tx\Rx)
3. The embedded device (Slave) receives the command from transmitter (Master).

4. The slave sends back the Tx command along with the synchronization counter.
5. The Master again send the command along with synchronization counter value and total count of the commands from Master.
6. The Slave device checks against the received value and performs the operation if it is a valid command value.

IV. SYSTEM IMPLEMENTATION AND OPERATION

The demonstrator project considers 8 peripherals (4 lights and 4 more house hold equipment's),

The demonstrator project considers 8 peripherals (4 lights and 4 more house hold equipment's), of which 4 light controls are implemented for demonstration purpose.

The 4 lights are controlled by a custom App runs on hand held device (Android based smart phone - Control master), which synchronizes with Peripheral master using Bluetooth protocol. The hand held device commands the peripheral master to control the peripherals using simple commands.

Dual Synchronization algorithm in use:

Both Master control and Peripheral control device runs synchronization counters from 1-4

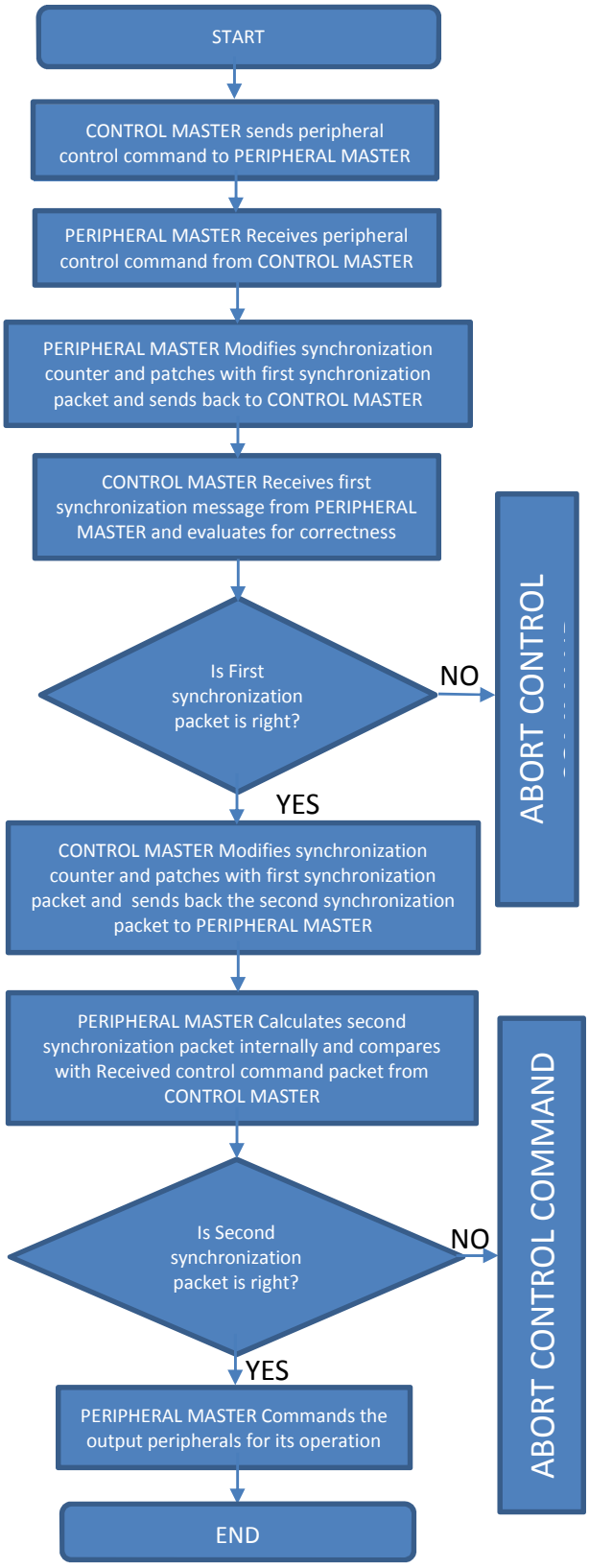
Use case1:

1. Control master sends command 1 to control light 1 & increment the sync counter 2.
2. Peripheral master receives command and increments sync counter to 2, and sends back value 3 (1+2) to control master.
3. The control master checks received value against internally calculated value (1+2) if matches, then sends the value 7 (3+4, value + total command count for 4 peripheral)
4. The Peripheral master receives value 7&subtracts counter value and total command count value (4) from received value (7-2-4 = 1), and performs operation based on the resulted command, in this case it is light 1.

Use case2: (subsequent operation)

1. Control master sends command 3 to control light 3& increment the sync counterto 3.
2. Peripheral master receives command and increments sync counter to 3, and sends back value 6 (3+3) to control master.
3. The control master checks received value against internally calculated value (3+3) if matches, then sends the value 10 (6+4, value + total command count for 4 peripheral).
4. The Peripheral master receives value 10 & subtracts counter value & total command count number (4) from received value (10-2-4 = 3), and performs operation based on the resulted command, in this case it is light 3.

V. CONTROL FLOW CHART



VI. HARDWARE SPECIFICATION OF DEMONSTRATOR PROJECT

Wpan (802.15.4), WiMAX (802.16e). Wireless USB.

Arduino uno[5] board fig(e)and IDE C programming

language

HC05 module fig(i)spp module (csr(California Silicon Radio) bluecore 04-external single chip Bluetooth system with cmos technology)

A relay, fig(f) switch

VII. ADVANTAGES

The IoT is an advanced concept to connect the devices remotely and shall be controlled.

The entire IoT concept with wireless connectivity is highly configurable with little software changes, which can be adopted to different applications, like Smart cities, smart transportation, Agricultural automation.

Bluetooth is a low cost wireless technology which is widely used in electronic devices. It is also energy efficient.

Using Bluetooth, data can be transmitted fasterat around 2 mbps speed.

Instead of using ir remotes or rf remotes a multipurpose devices can be configured for control purpose, E.g. smartphones.

Reduces wiring harnesses and physical connectivity switch boards not required

VIII. LIMITATIONS OF DEMONSTRATOR PROJECT

Cyber and embedded security is a critical factor for the IoT applications. There is need for stronger and multi-level security algorithms for complex systems like nuclear power plant controls to protect the system.

Cyber and embedded security is a critical factor for the IoT applications. There is need for strongerand multi-level security algorithms for complex systems like nuclear power plant controls to protect the system.

Improper encryption can lead to unauthorized access to wireless commands.

Using Bluetooth, we can only connect to devices within the range of 10 mts.

The speed of execution is reduced due to dual acknowledge mechanism of protocol security.

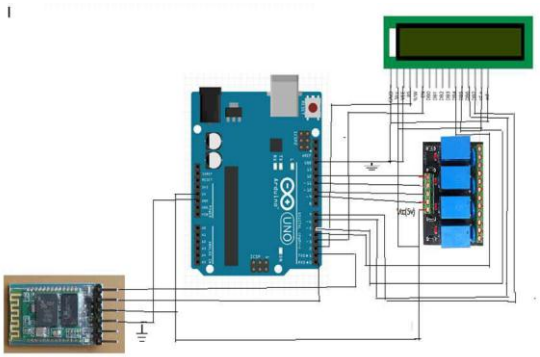
IX. RESULTS AND CONCLUSION

The demonstrator project exercises the basic security algorithm built on a dynamic behavior of the system from booth peripheral control modules and Master control module, which eliminated most of the hacking problems.

The industries and entire eco system is moving towards Internet of Things adaptation for larger, integrated and remote applications. The applications ranging from simple home automation system, traffic management to controlling of power grids, nuclear power plants, which demands a greater security challenges. The most dynamic and non-predictable algorithms will be future need for secure communication.

X. INTERFACING DIAGRAM

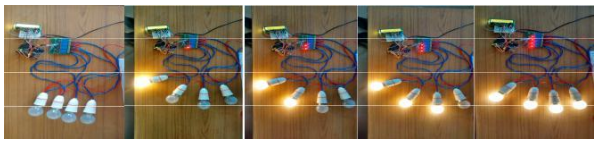
Fig(a)



XI. ANDROID APP IMAGE

Fig(b)

Fig(c)



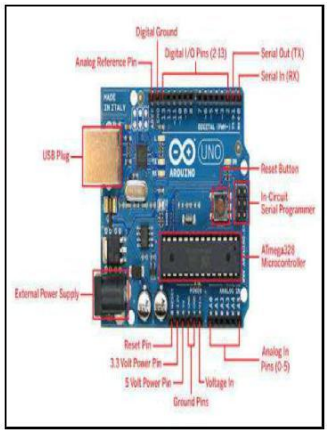
XIII. SPECIFICATION AND WIRING IMAGES

Fig(d)

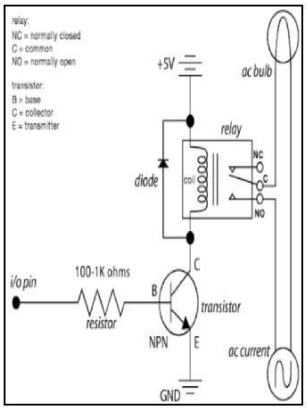
Technical specs

Microcontroller	ATmega328P
Operating Voltage	5V
Input Voltage (recommended)	7-12V
Input Voltage (limit)	6-20V
Digital I/O Pins	14 (of which 6 provide PWM output)
PWM Digital I/O Pins	6
Analog Input Pins	6
DC Current per I/O Pin	20 mA
DC Current for 3.3V Pin	50 mA
Flash Memory	32 KB (ATmega328P) of which 0.5 KB used by bootloader
SRAM	2 KB (ATmega328P)
EEPROM	1 KB (ATmega328P)
Clock Speed	16 MHz
Length	68.6 mm
Width	53.4 mm
Weight	25 g

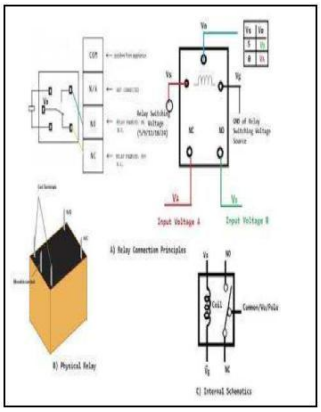
Fig(e)



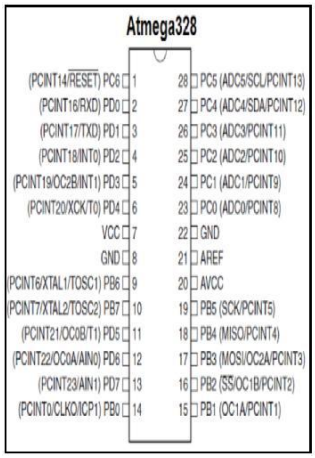
Fig(f)



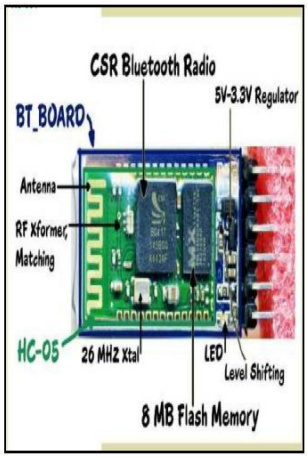
Fig(g)



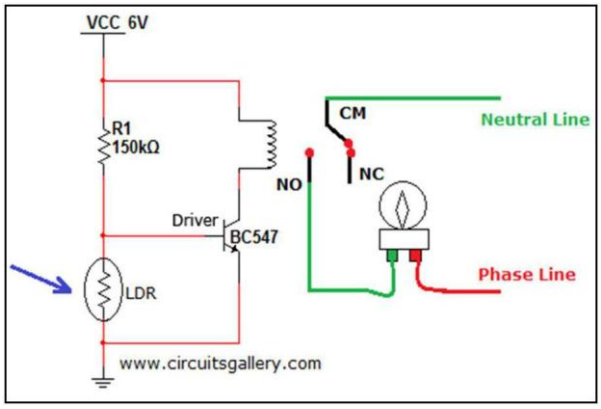
Fig(h)



Fig(i)



Fig(j)



XIV. REFERENCES

[1] Books: internet of things with the arduino yun by macro Schwartz, Arduino uno:a hands on guide for beginner by aguskurniawan

[2] Smart home system via Wireless Bluetooth y R. A. Ramlee; D. H. Z. Tang; M. M. Ismail System Engineering and Technology (ICSET), Year: 2012

[3] Electrical home appliances control system over Bluetooth with android by H. Kanma; N. Wakabayashi; R. Kanazawa; H. Ito IEEE Transactions on Consumer Electronics Year: 2003

[4] Bluetooth technology a viable solution for IoT by Kuor-Hsin Chang IEEE Wireless CommunicationsYear:2004

[5] Arduino Uno to digital control of power electronics Lukas Müller; Masihuddin Mohammed; Jonathan W. Kimb all, Year: 2015

[6] The Capacity of Relay Channels. Hon-Fah Chong; MehulMotani IEEE Transactions on Information Theory, Year: 2011

[7] Websites:
arduino.cc, engineers garage.com, electronicshub.org,electronicsforu.com, m.instructables.com