Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 165 (2019) 421–427

Procedia Computer Science

www.elsevier.com/locate/procedia

INTERNATIONAL CONFERENCE ON RECENT TRENDS IN ADVANCED COMPUTING 2019, ICRTAC 2019

REMOVING RF VULNERABILITIES FROM IOT DEVICES

Pranab Ray*, Parveen Sultana H, Sushmita Ghosh

Vellore Institute of Technology Vellore 632014,India

Abstract

RF vulnerabilities is a massive problem nowadays. If you see TV remote, AC remote, camera and car remotes RF have been using everywhere. The problem with RF security is that it always generates a signal with the same key which locked or unlock the system. RF signals are also unencrypted and It transfers signal through an unsecured channel so It suffers from key relay attack where the same key signal used to generate every time from a captured RF signal having the same key to make work to the system. Our problem statement is "Removing RF vulnerabilities to transfer data securely so that RF can avoid any types of relay attack threats". we proposed a system which transferred data securely, In our system, we advise key rolling algorithm with a 2-way handshake**,** Key rolling algorithm rolls key which provides a new key every time of data transferring and 2-way handshaking provide synchronization between sender and receiver.

Keywords: Radio frequency (RF) ; key rolling algorithm; 3 way handshaking;Acknowledgment (ACK); Synchronized (SYN) ;Television(TV);Air conditioning(AC);A random secret unique code (Key).

* Corresponding author. Tel.: +9-630-265-2355;.
E-mail address: pranabray04@gmail.com

10.1016/j.procs.2020.01.001

1. Introduction

The era of the Internet of Things, where digitally connected devices are infringing on each perspective of our lives, counting our homes, workplaces, cars and indeed our bodies.

These devices are securely interconnected via various wireless technologies like radio. One of them is Radio Frequency(RF) which is used for wireless transmissions among the IOT devices. IoT brings with it an increment within the request for remote innovations.RF emits from the source antenna and travels to the receiver's antenna. And the data is modulated from to source side to receiver's side wirelessly. This wireless technology for transferring of data between devices is vulnerable to various attacks which can easily harm the system.

RF[2] uses same key every time for the data transfer which is very unsafe channel. These channels are unsafe for the transmission for data sa it is not encrypted so it can be easily attacked by a third party which can lead to data tampering, evans dropping etc. Therefore, we need to add security to this transmission channel by using key rolling algorithm.

Key rolling algorithm[1] is used for secure data transmission. It uses every time new key for each transmission of data which makes it more secure than the previous mentioned method. This algorithm uses key from the key set and transmits the data and then data is received on the other end. Receiver uses the same key to get access to the data. Now if the sender want to again send some data

then it will user another key from the key set. The key may be repeat after a particular interval of time.

Along with this we have also used 2 way handshaking which is used for secure connection. The sender will first send the receiver a request for the data transmission and then the receiver will allow it, after that the sender can send data . This makes the system secure from many vulnerabilities like fraud connection, repudiation etc.In this paper, we introduced a method for secure data transmission in IOT devices using key rolling algorithm with 3 way handshaking which prevents the system from various attacks.

1.1. Literature Review

An early study for a key rolling algorithm by ATMEL[1] depicts a Secure Rolling Code Algorithm transmission convention for utilizing in a unidirectional remote communication framework. This scheme guarantees that ancient messages are never acknowledged unless the head of the rolling window has come to the old counter values. No transmission is ever repeated which avoids a would-be cheat from snatching the message and retransmitting and It is essentially outlandish to anticipate message substance, indeed in the event that past messages are known. The collector disregards all messages that have as of now been used.

The work of Guangyu Zhu and Gul N. Khan, (2013)[3] shows a securely shared authentication convention for RFID frameworks that are based on a symmetric key procedure with a proficient key upgrading instrument. They have given a strategy to progress the RFID framework security against various assaults. The method by creating a subkey and its index is up. The confirmation convention includes a tall level of security against replay, spying, and man-in-the-middle assaults. It too has moo computation and communication costs.

In the field of the study of TCP/ IP, the creators gave the visualization of working of three-way handshake of

TCP/IP[4] utilizing perception of the 3-way handshake with OpenGL utilizing Microsoft Visual C++. The inquire about has entirely spoken to the stream of parcels in an organized[5]
and the different angle that challenges to it. An exhibit of three-way handshake all the things from effective sending to bundle misfortune as well as the acknowledgment sending and the misfortune is well illustrated[6]. There's moreover a timer appear to form the investigate look more realistic..
The work was done by Fu-Hau Hsu, Yan-Ling Hwang, Cheng-Yu Tsai, Wei-Tai Cai, Chia-Hao Lee 1, and KaiWei Chang ,(2016)[7] deals on assaults that expend all the transmission capacity accessible to the casualty machine. Whereas concentrating on the transmission capacity assault the TCP SYN surge is the more unmistakable assault. TCP particular testing is utilized within the proposed conspire where the client is asked to alter the windows estimate/ cause parcel retransmission while sending the ACK within the three-way handshake. Usually exceptionally valuable to discover the Spoofed IP Packets/TCP SYN surge and avoiding them.

1.2. Related Work

For the secure data transmission wirelessly, the technology which is mostly used is radio transmission. The existing system uses the unsecure channels to send the data which is very risky which invites vulnerable attacks. The work done by Guangyu Zhu and Gul N. Khan[3], their objective is to improve the RFID system security against replay, de-synchronization, eavesdropping and man-in-the-middle attacks while maintaining lower computation, communication and storage and replay attack. Then the server encrypts it using KEY sys as the first message m0. Upon receiving m0. The tag encrypts its ID using the current secret keyset KEY n . The encrypted ID is cover-coded with the new subkey from m0. The computation result is sent as message m1.m2 is the expected reply.

The key rolling algorithm uses the symmetric keys in the both sides of sender and receiver for data accessing. It uses every time new key for each transmission. The key is stored in circular queue format so the after some particular interval the keys will repeat shown in figure 1.

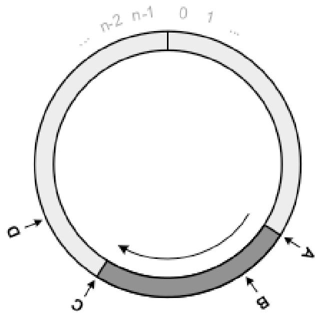


Figure.1 Rolling Key

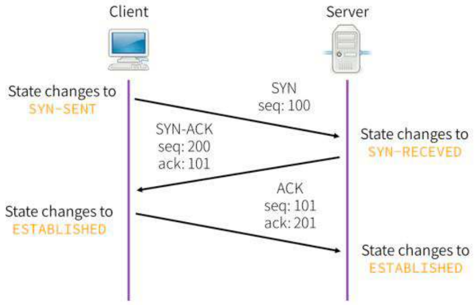


Figure. 2. 3-way handshaking

Here,
A- value stored for last key
B-counter key value(accepted)
C-end of slot

D-rejected values
The 3 way handshaking[7][4] will provide synchronisation between sender and receiver. In figure 2, the client/sender will send request for sending data. The server/receiver will then receive it and allow the sender to send data. Now, the connection will be established between the sender and the receiver. Then sender can send data over the channel.
It avoids the uninvited connections and repudiations in the networking of the IOT devices which makes the system more secure.

2. Methodology

We used key rolling algorithm and the 2 way handshake algorithm for secure data transfer.
The key rolling algorithm uses keys for the secure data transmission. The key values are made as set and stored in the circular queue. This key set is shared with the sender and receiver. When the data is transferred using this algorithm, then one of the blocks of the circular queue is selected as the key and stored. And to get access to the same data we have to use the key set in the receiver side when the selected key matches the set then it can be accessed.

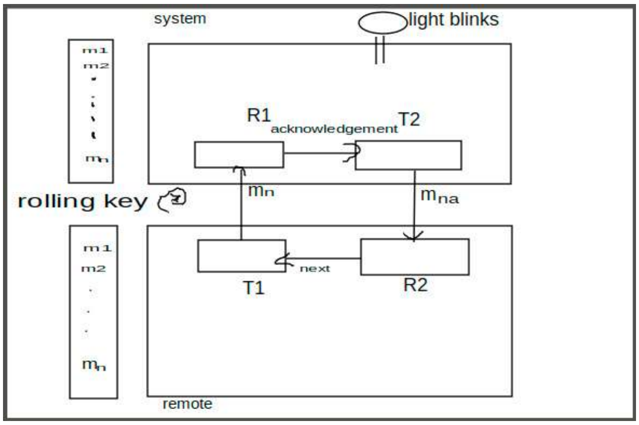


Figure. 3 shows Key rolling algorithm

The above Figure 3 is the system diagram of our approach. We have remote(sender) and door(receiver) in the above diagram . In the remote, we have T1(Rf Transmitter 1) , R2(Rf Receiver 2) and door have R1(Rf Receiver 1) and T2(Rf Transmitter 2).T2 and R2 used for acknowledgement.
Circular Queue is a straight data structure in which the operations are performed based on FIFO (To begin with In To begin with Out) guidelines and the last position is connected back to the primary position to form a circle. It is additionally called 'Ring Buffer'. It can be used for storing the keys for key rolling system efficiently. the same key can repeated or reused after some particular interval of time for the operation[9][8].
Utilizing a circular queue in this project gives several factors that make the encryption/decryption handle more

difficult for eavesdroppers to decode the ciphertext.

We have used 2 way handshaking to synchronize between sender and receiver which provides secure connection between them. Here, we will use concept like stop and wait protocol where after transmission of one message completely next message will be transferred if any desynchronization will be then the whole system will be reset. That's the main advantage of our approach method.

The system is designed with double click.

1. *every time system used to play different key.*

we took a set of keys where sequence of keys in both sender and receiver are equal.when we click button at sender side it send key to receiver.We used circular queue in sender and receiver side. We used key side sequence as ‘abcdefghijklm’ where as receiver side also uses the same sequence.

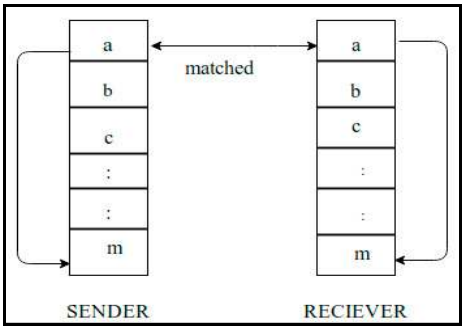


Figure 4 synchronization algorithm circular queue

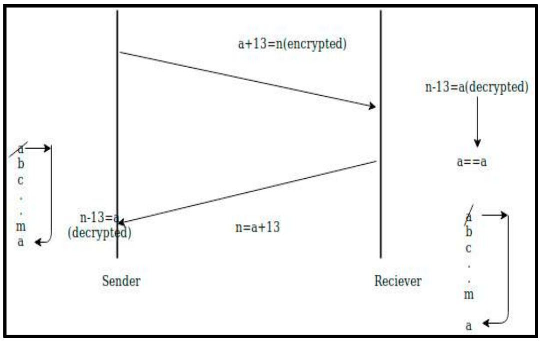


Figure. 5 Encryption with key

Above Figure. 4 shows the basic algorithm for our proposed system. It shows the working of the circular queue with the key rolling algorithm

2. *Synchronization of the system.*

we used two way handshaking .Sender sends key but do not remove from its queue unless it get acknowledgement from the receiver . Above all we have used shift shift cipher encryption .In the below Figure. 5 we have shown our 2-way synchronization and encryption mechanization. Sender sends encrypted messages with the shift key of 13,After encryption the encrypted key will be ‘n’.When receiver will receive the encrypted key ‘n’ it decrypt to normal plain key ‘a’.The received decrypted plain key is buffered and checked with the top of the queue key if it matches then the top of the queue is removed and send a acknowledgement signal of removing key from sender side.

First test cases if receiver does not receive the signal then no removal of key with no hand shaking. Second Test case if sender does not receive ack signal then nothing is going to happen ,the key ‘a’ from the sender side queue will not remove.

3. Experiments and results

Here, we took two arduino with two transmitter and two receiver shown in the Figure. 6

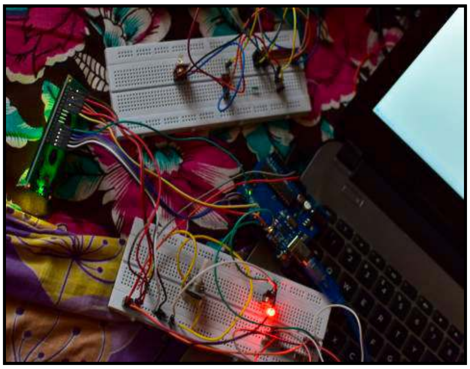
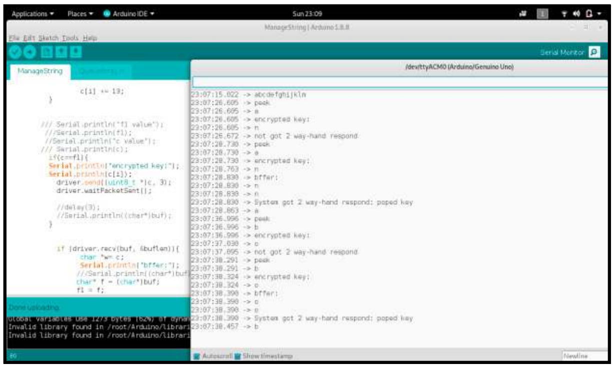


Figure 6 Full System



```
        c[i] += 13;
    }

 /// Serial.println("f1 value");
  //Serial.println(f1);
  //Serial.println("c value");
 /// Serial.println(c);
  if(c==f1){
  Serial.println("encrypted key:");
  Serial.println(c[i]);
    driver.send((uint8_t *)c, 3);
    driver.waitPacketSent();

    //delay(3);
    //Serial.println((char*)buf);
  }

    if (driver.recv(buf, &buflen)){
        char *w= c;
        Serial.println("bffer:");
       ///Serial.println((char*)buf
       char* f = (char*)buf;
       f1 = f;
```

```
Done uploading.
Global variables use 1273 bytes (62%) of dynam
Invalid library found in /root/Arduino/librari
Invalid library found in /root/Arduino/librari
80
```

```
23:07:15.822 -> abcdefghijklm
23:07:26.605 -> peek
23:07:26.605 -> a
23:07:26.605 -> encrypted key:
23:07:26.605 -> n
23:07:26.672 -> not got 2 way-hand respond
23:07:28.730 -> peek
23:07:28.730 -> a
23:07:28.730 -> encrypted key:
23:07:28.763 -> n
23:07:28.830 -> bffer:
23:07:28.830 -> n
23:07:28.830 -> n
23:07:28.830 -> System got 2 way-hand respond: poped key
23:07:28.863 -> a
23:07:36.996 -> peek
23:07:36.996 -> b
23:07:36.996 -> encrypted key:
23:07:37.030 -> o
23:07:37.095 -> not got 2 way-hand respond
23:07:38.291 -> peek
23:07:38.291 -> b
23:07:38.324 -> encrypted key:
23:07:38.324 -> o
23:07:38.390 -> bffer:
23:07:38.390 -> o
23:07:38.390 -> o
23:07:38.390 -> System got 2 way-hand respond: poped key
23:07:38.457 -> b
```

Figure 7

In the figure 7 this is first phase when we click button afterwards sender encrypts key and send it.After sending key it waits for handshaking.

The system got unlocked after clicking the button.given below in figure 8. It send feedback(acknowledgement) signal to sender at same time.The signal is stored in the buffer of sender(T1).

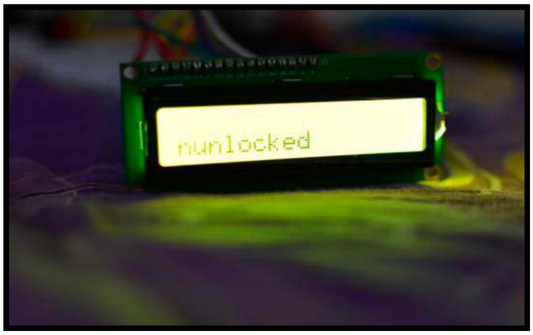
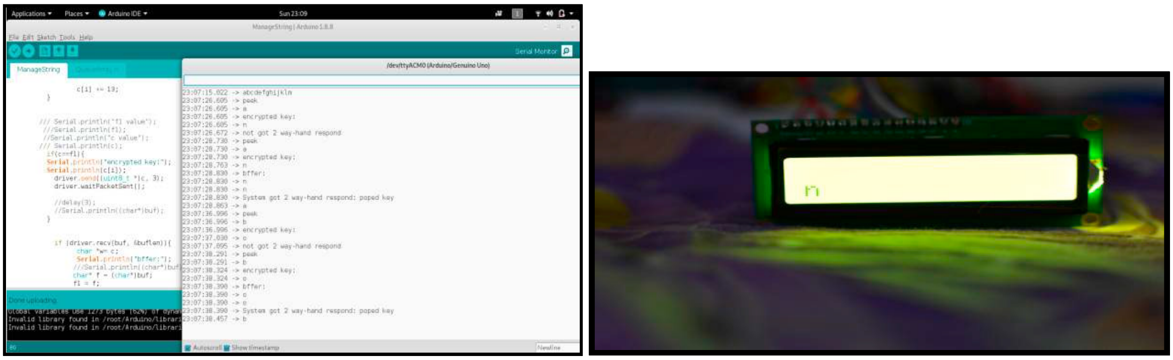


Figure 8 Display with unlocked State

When we click next time the key stored in the buffer get matched with the peek of the queue if it is same then we pop the key from the queue which implies 2-way hand shaking.



```
        c[i] += 13;
    }

 /// Serial.println("f1 value");
  //Serial.println(f1);
  //Serial.println("c value");
 /// Serial.println(c);
  if(c==f1){
  Serial.println("encrypted key:");
  Serial.println(c[i]);
    driver.send((uint8_t *)c, 3);
    driver.waitPacketSent();

    //delay(3);
    //Serial.println((char*)buf);
  }

    if (driver.recv(buf, &buflen)){
        char *w= c;
        Serial.println("bffer:");
       ///Serial.println((char*)buf
       char* f = (char*)buf;
       f1 = f;
```

```
Done uploading.
Global variables use 1273 bytes (62%) of dynam
Invalid library found in /root/Arduino/librari
Invalid library found in /root/Arduino/librari
80
```

```
23:07:15.822 -> abcdefghijklm
23:07:26.605 -> peek
23:07:26.605 -> a
23:07:26.605 -> encrypted key:
23:07:26.605 -> n
23:07:26.672 -> not got 2 way-hand respond
23:07:28.730 -> peek
23:07:28.730 -> a
23:07:28.730 -> encrypted key:
23:07:28.763 -> n
23:07:28.830 -> bffer:
23:07:28.830 -> n
23:07:28.830 -> n
23:07:28.830 -> System got 2 way-hand respond: poped key
23:07:28.863 -> a
23:07:36.996 -> peek
23:07:36.996 -> b
23:07:36.996 -> encrypted key:
23:07:37.030 -> o
23:07:37.095 -> not got 2 way-hand respond
23:07:38.291 -> peek
23:07:38.291 -> b
23:07:38.324 -> encrypted key:
23:07:38.324 -> o
23:07:38.390 -> bffer:
23:07:38.390 -> o
23:07:38.390 -> o
23:07:38.390 -> System got 2 way-hand respond: poped key
23:07:38.457 -> b
```

Figure. 9 (a) exection screen; (b) display ‘n’.

In the above figure 9 a) and b) the encrypted key value is shown when the receiver .This is shown in our system when receiver side of key received acknowledgement .

4. Conclusion

The approached method successfully rolls the key over the every transmission. The key rolling algorithm provides high security by using different keys every time which prevents the system from the vulnerable attacks like masquerading , data tampering evance dropping, etc. Whereas the 2-way handshaking makes sure the secure connection before the transmission of the data all over the session,here 2-way helps to synchronize between sender and reciver so that any one can not dis-syncronized the communications or if any one did also then a new communication sessions will start.

References

[1] "Secure Rolling Code Algorithm for Wireless Link"(2015) ,AVR411, application notes, Atmel,2600E–AVR–07/15

[2] Elvis Babačić,Zoran Veljović,Milica Pejanović-Đurišić, (2017)"Radio-frequency spectrum management in wireless IoT networks" ,

[3] Guangyu Zhu and Gul N. Khan, (2013) "Symmetric key based RFID authentication protocol with a secure key-updating scheme",

[4] Usha Rani J , Madhu M Nayak, Anandhi G (2017), "Visualization of Three Way Handshake Mechanism", Volume 5 Issue V, ISSN: 2321-9653

[5] L.Kavisankar, C.Chellappan,(2011),"A Mitigation model for TCP SYN flooding with IP Spoofing".International Conference on Recent Trends in Information Technology, ICRTIT, 251-256

[6] Yoon-Su Jeong,Yoon-Cheol Hwang,Ning Sun, Ki-Su Kim, Sang-Ho Lee,(2007), "RFID Authentication Protocol using Synchronized Secret Information", IEEE, First International Symposium on Data, Privacy and E-Commerce,459-462

[7] Fu-Hau Hsu , Yan-Ling Hwang , Cheng-Yu Tsai , Wei-Tai Cai , Chia-Hao Lee 1, and KaiWei Chang ,(2016) "TRAP: A Three-Way Handshake Server for TCP Connection Establishment", applied sciences, Journal of Supercomputing, Volume 72, Issue *1*, 120-140

[8] Ali N. Albu-Rghaif , Abbood Kirebut Jassim , Ali J. Abboud,(2018), "A data structure encryption algorithm based on circular queue to enhance data security", 3 Scientific Conference of Engineering Science (ISCES), 24-29

[9] S. Phull and S. Som,(2016) "Symmetric Cryptography using Multiple Access Circular Queues (MACQ)", Proceedings of the Second International Conference on Information and Communication