An Improved Novel Key Management Protocol for RFID Systems

Rania Baashirah, BVenkata Tarun Varma Namburi, Chakradhar Polisett, Naresh Ravuri,
Vinay Kumar Avula, and Shakour Abuzneid
Department of Computer Science & Engineering
University of Bridgeport, Bridgeport, CT

Abstract

The growing demand to organize resourceful ways of identification has made "Radio Frequency Identification (RFID)" technology universal. One of the key problems in RFID is security and privacy. Many RFID authentication protocols have been proposed to preserve security and privacy of the system. Nevertheless, most of these protocols are analyzed, and it is shown that they cannot provide security against some RFID attacks. In this paper, we present a novel cryptographic scheme, "Hacker Proof Authentication Protocol (HPAP)" which has been improved for "Multiple Tags" authentication at a single time process. We simulated the system using Java Application, and it is a time-saving process. Simulation using Java shows our protocol is secure with the fastest updating timestamps.

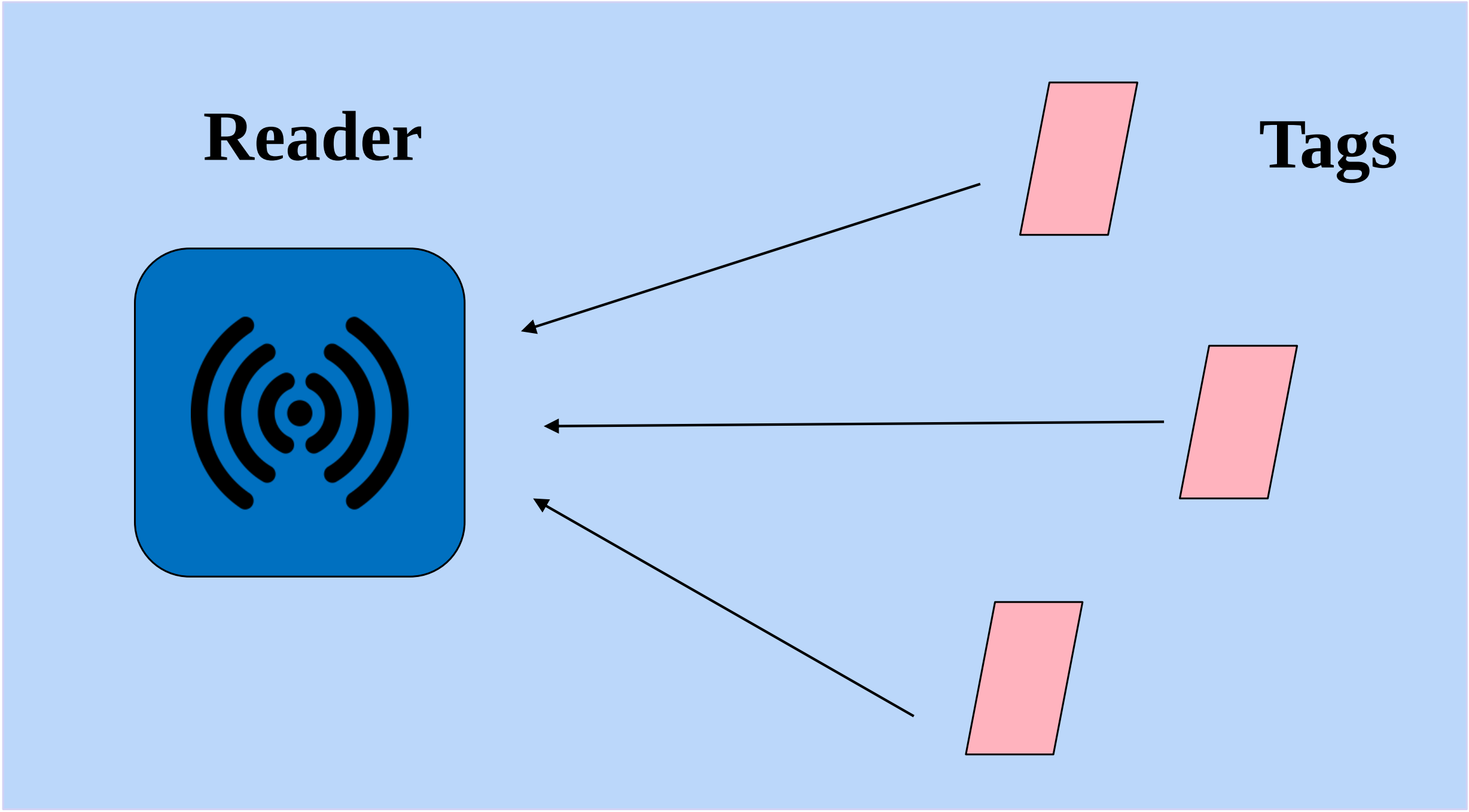
HPAP

The protocol is proposed by Hakeem et al. in 2013. The main is to maintain confidentiality, integrity, and security against different attacks using cryptographic authentication protocols for efficient RFID system. The protocol is based on the use of timestamp, lightweight hash function, and pseudo-random number generator (PRNG). The protocol is proved to be secure against:

- Replay attack
- Tag impersonation
- Tracking
- Location privacy
- Information leakage
- Man-In-The-Middle
- Message interception
- DOS attack
- De-Synchronization

Multi-Tag HPAP

HPAP protocol was proposed to authenticate only one tag in the system. We extended the work to simulate the protocol and improve it by eliminating all its error and make it more efficient to authentication multiple tags for one reader signal.

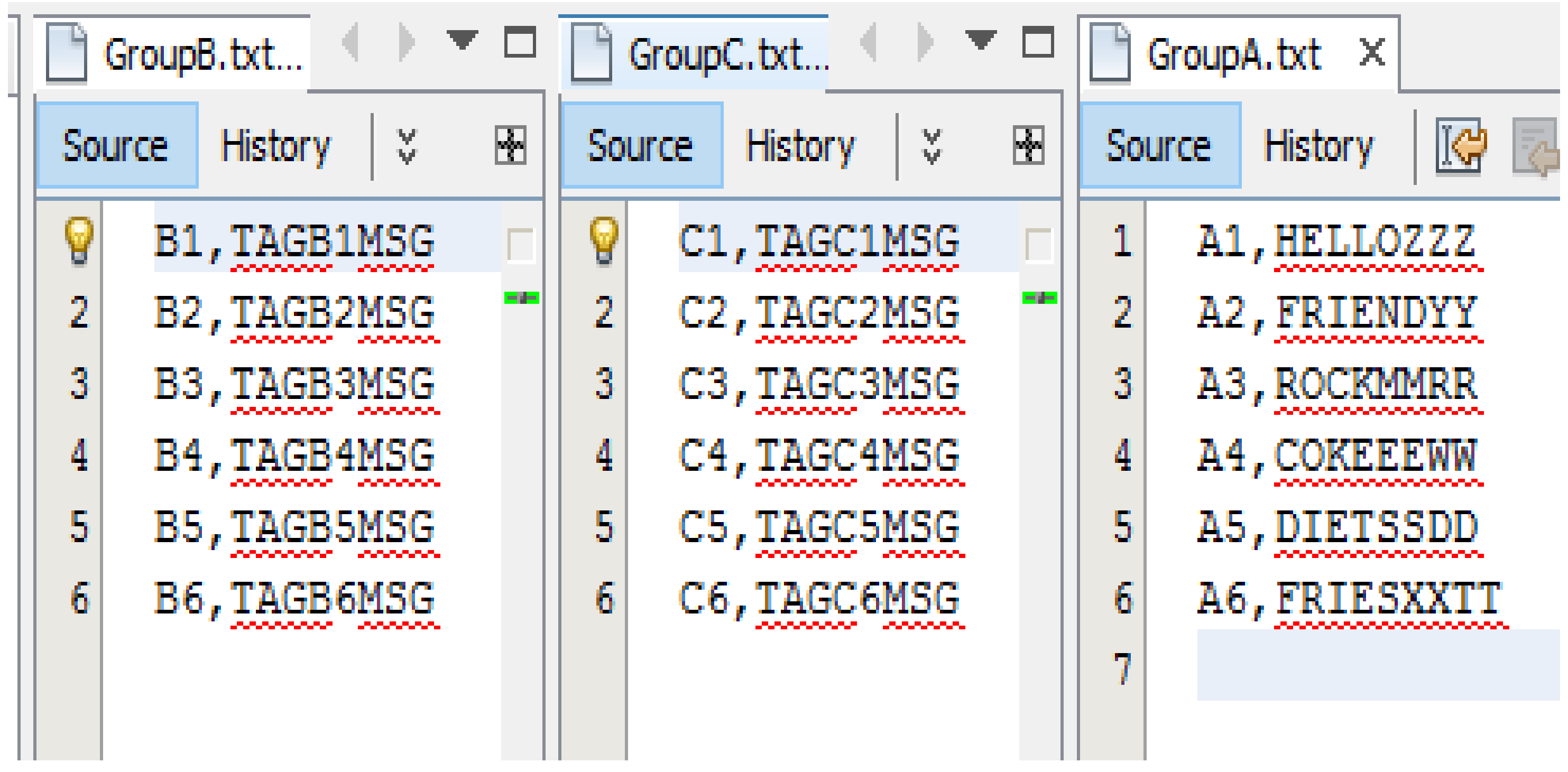


Implementation

Java code simulation is done using Net beans IDE. We tested the protocol for three groups Group-A, Group-B, Group-C with six tags in each group that are stored in .txt files.

HPAP Functions:

1. File IO system
2. Hash Map
3. Date and Calendar
4. Random
5. Print
6. Scanner

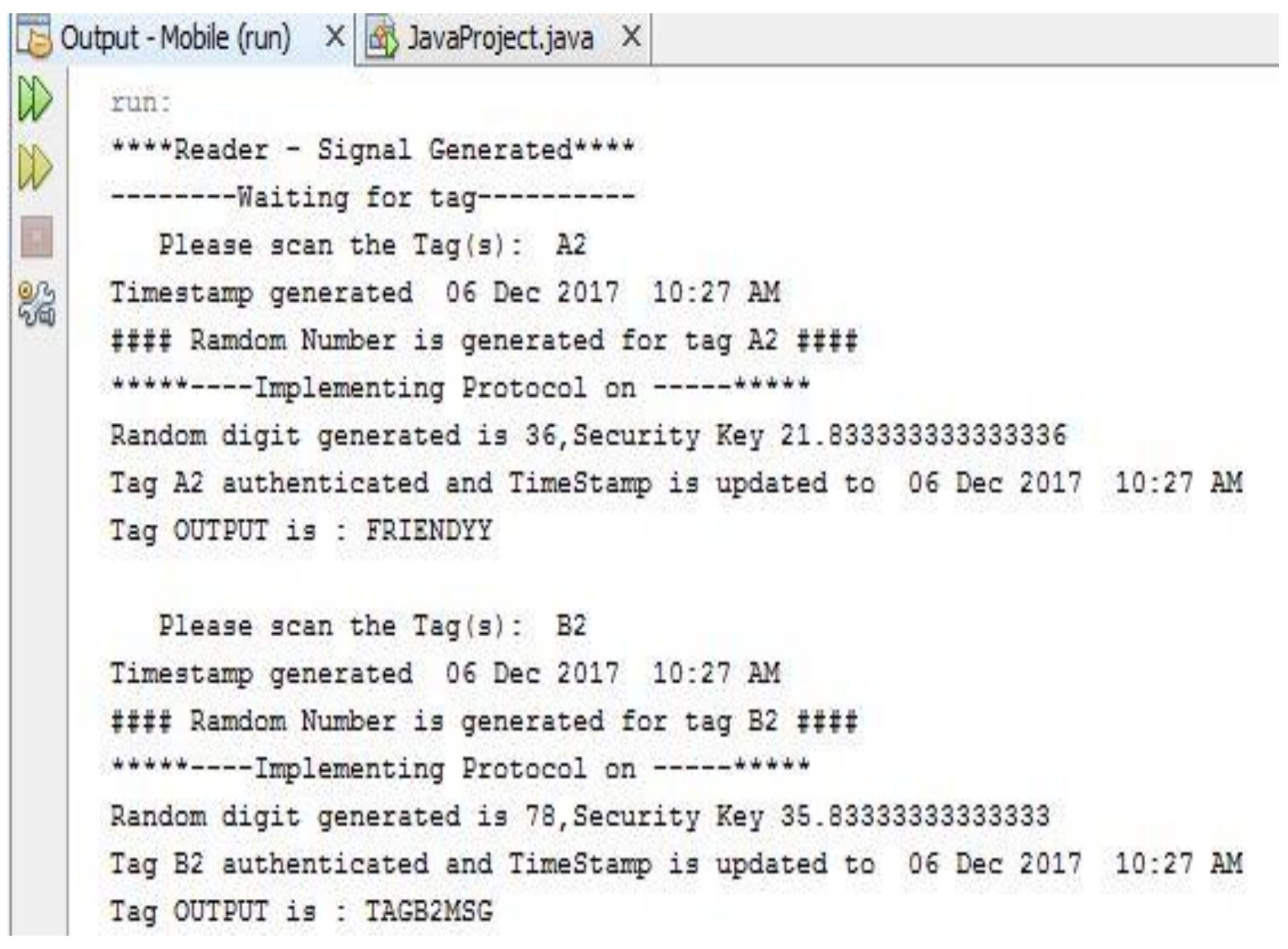


```
B1,TAGB1MSG
B2,TAGB2MSG
B3,TAGB3MSG
B4,TAGB4MSG
B5,TAGB5MSG
B6,TAGB6MSG
```

```
C1,TAGC1MSG
C2,TAGC2MSG
C3,TAGC3MSG
C4,TAGC4MSG
C5,TAGC5MSG
C6,TAGC6MSG
```

```
A1,HELLOZZZ
A2,FRIENDYY
A3,ROCKMMRR
A4,COKEEEWW
A5,DIETSSDD
A6,FRIESXXTT
```

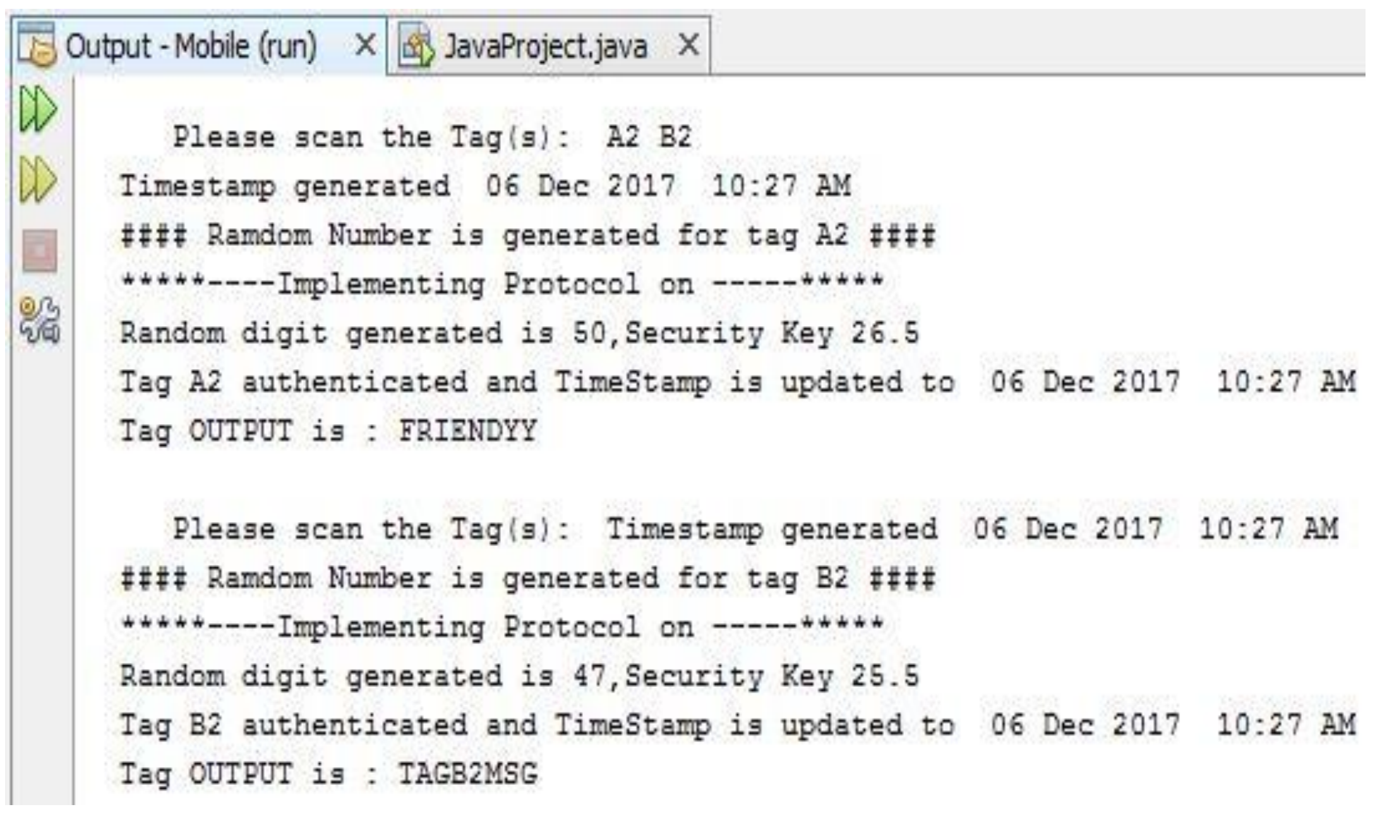
Results



```
run:
****Reader - Signal Generated****
--------Waiting for tag----------
   Please scan the Tag(s):  A2
Timestamp generated  06 Dec 2017  10:27 AM
#### Ramdom Number is generated for tag A2 ####
*****----Implementing Protocol on -----*****
Random digit generated is 36,Security Key 21.833333333333336
Tag A2 authenticated and TimeStamp is updated to  06 Dec 2017  10:27 AM
Tag OUTPUT is : FRIENDYY

   Please scan the Tag(s):  B2
Timestamp generated  06 Dec 2017  10:27 AM
#### Ramdom Number is generated for tag B2 ####
*****----Implementing Protocol on -----*****
Random digit generated is 78,Security Key 35.83333333333333
Tag B2 authenticated and TimeStamp is updated to  06 Dec 2017  10:27 AM
Tag OUTPUT is : TAGB2MSG
```

Single-Tag



```
   Please scan the Tag(s):  A2 B2
Timestamp generated  06 Dec 2017  10:27 AM
#### Ramdom Number is generated for tag A2 ####
*****----Implementing Protocol on -----*****
Random digit generated is 50,Security Key 26.5
Tag A2 authenticated and TimeStamp is updated to  06 Dec 2017  10:27 AM
Tag OUTPUT is : FRIENDYY

   Please scan the Tag(s):  Timestamp generated  06 Dec 2017  10:27 AM
#### Ramdom Number is generated for tag B2 ####
*****----Implementing Protocol on -----*****
Random digit generated is 47,Security Key 25.5
Tag B2 authenticated and TimeStamp is updated to  06 Dec 2017  10:27 AM
Tag OUTPUT is : TAGB2MSG
```

Multi-Tag

Conclusion

The ubiquitous implementation of RFID systems in various applications has encouraged us to develop strong authentication protocols for privacy and security. In this paper, we have proposed a new cryptographic mutual authentication protocol in which a timestamp and pseudo-randomize update is presented. The updates on the secret value of the tag and encryption key are done by using an algorithm. This HPAP protocol is limited to a single tag. Only one tag can be authenticated for one reader signal. We improved this protocol to be able to authenticate multi tags per one reader signal before terminating the signal. This protocol eliminates all the attacks by generating a unique random number for every tag. This random number is used to create a secret key from an algorithm. We have used the same algorithm presented in the protocol. The communication cost between the tag and the server is reduced in our protocol resulting in lower cost of the whole system. Also, the Authentication is securely done in no time which is a major development.