lasaris LAB OF SOFTWARE ARCHITECTURES AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
Masaryk University

Self-adaptive RFID Authentication for Internet of Things

Bacem Mbarek, Ph.D.

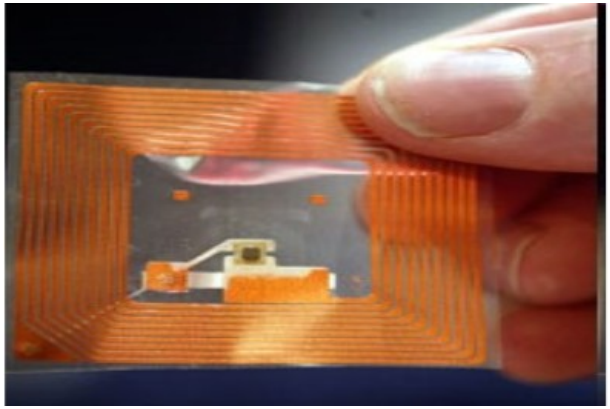
Masaryk University, Czech Republic
Lasaris Lab (Lab of Software Architectures and Information Systems)

PLAN

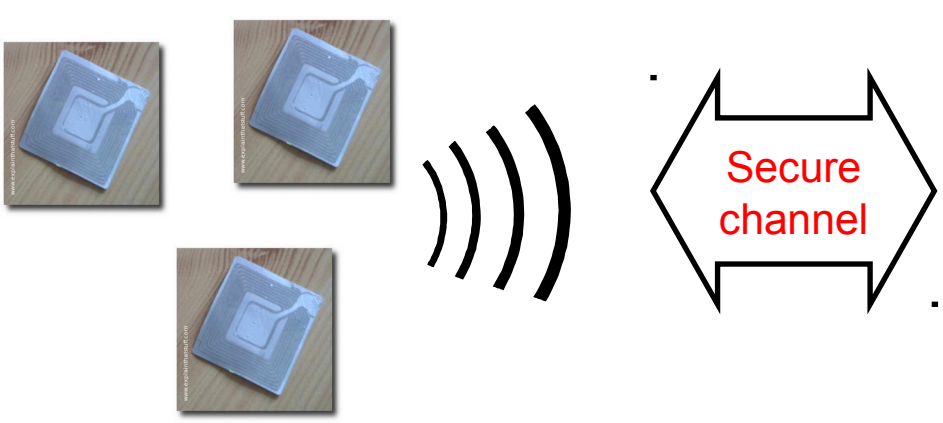
1. Introduction
2. Problematic and Goals
3. Contributions
4. Conclusion & Future works

what, really, is “RFID”?

- Radio frequency identification (RFID) is an automatic identification method,
- Retrieve and access data using RFID tags
- RFID tags are intelligent bar codes that can talk to a networked system which can track and identify every product using radio waves,
- RFID system includes:
  - Tags, readers, database system
- RFID tags are small, wireless devices that help identify objects and people.



Authentication for RFID Systems

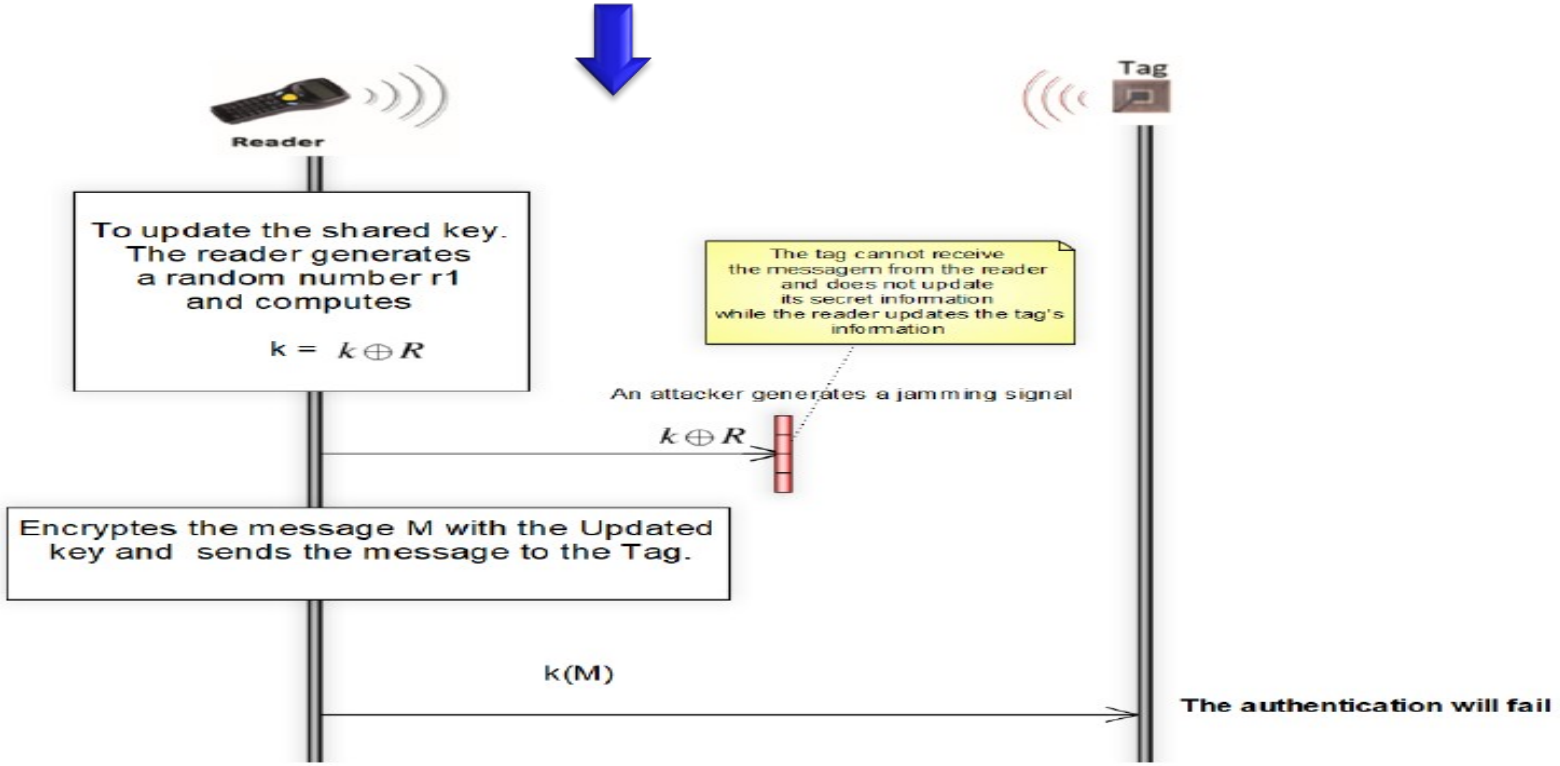


Tags

Reader

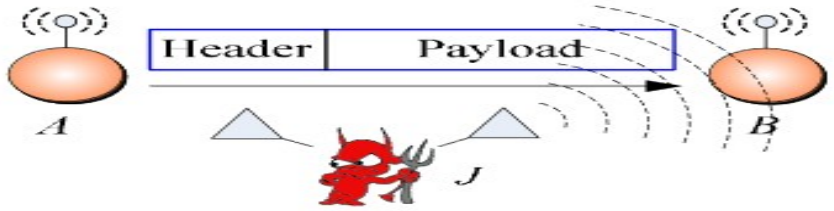
Jamming attack

Due to the lack of efficient key updating algorithms, previous schemes are vulnerable to **jamming attacks**.



Update of keys and Jamming attacks

- An attacker generates a jamming signal



- The tag cannot receive the message from the reader and does not update its secret information while the reader updates the tag's secret information.

➡ **After this attack, the secret information will be inconsistent between the reader and the tag. Therefore, the authentication will fail.**

Jamming attack and keys update

1

If the adversary compromises some tags, however, it obtains several paths from the root to those leaf nodes of the compromised tags,
as well as the keys on those paths. Since keys are never changed in the static

2

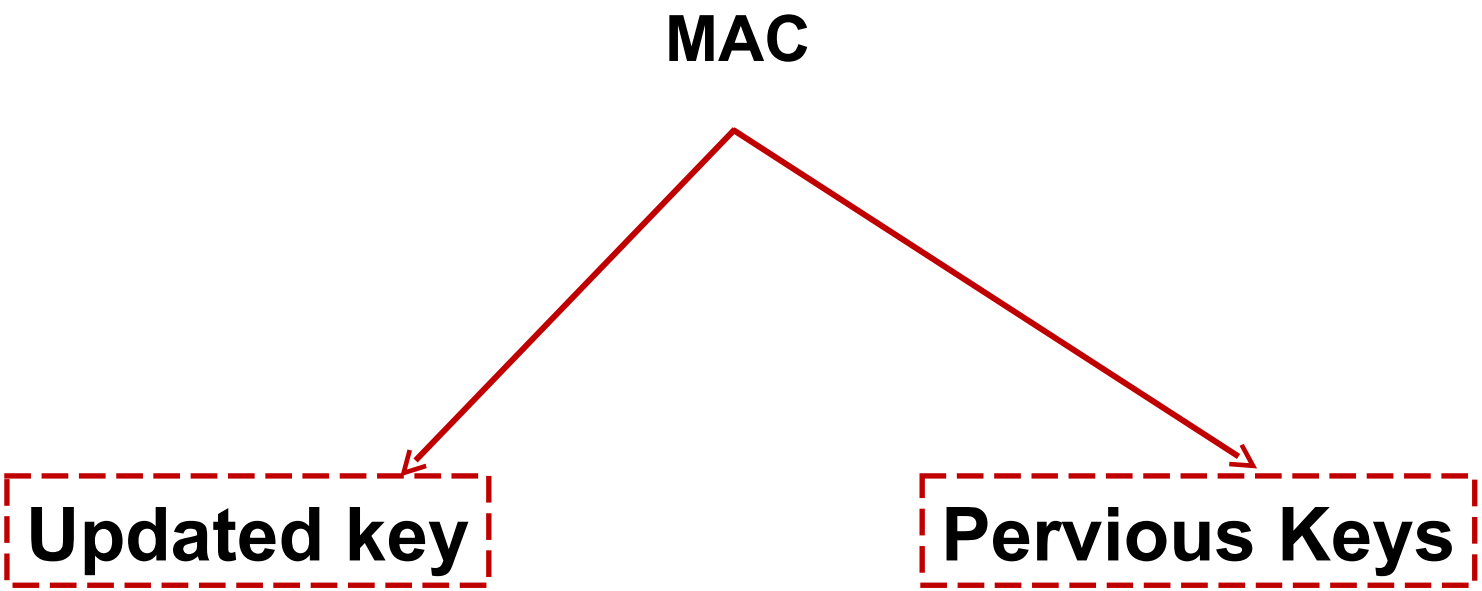
A practical solution is to update keys for a tag after each authentication so that the adversary cannot make use of keys obtained from compromised tags to attack uncompromised ones.

Contribution

- we have proposed a new self-adaptive RFID authentication protocol, named as SAM, to provide a secure and efficient tag-to-reader transaction in IoT applications.
- By using dynamic key-updating algorithms, our proposed solution enhances the key updating system based on enabling different ways to authenticate packets, which significantly reduces the impact of jamming attacks.
- One important advantage of our protocol is that it can be seamlessly deployed to existing systems for increasing the security of tag identification while at the same time maintaining the system efficiency.

Contribution

The reader appends MACs with different keys,



Contribution

The first algorithm describes the different authentication steps done by the reader.

Algorithm 1 Authentication Procedure on the Reader

The reader generates a random value R and computes $k = k \oplus R$
if $k \oplus R$ is not unique **then**
  the reader regenerates R until $k \oplus R$ becomes unique.
else if $k \oplus R$ is unique **then**
  Server encrypts the updated key with the previous key $K_i(k_{updated})$ and sends it to the tag.
  if update keys are lost due to packet loss or jamming attacks. **then**
    The reader can communicate with the tag using N previous keys.
    The reader creates and sends the following structure to the tag.
    $S = < k_{updated}(M) || k_i(M), k_{i-1}(M), ..., k_{i-N+1}(M) >$
  end if
end if

Contribution

If some disclosed keys are lost due to packet loss or jamming attacks, the tag still can recover the key from the previous keys and check the authenticity of messages.

Algorithm 2 Authentication Procedure on the Tag

The Tag checks $K_{updated}(M)$
if it is correct **then**
  The reader is authenticated.
else if it is not correct **then**
  Tag checks $k_i(M), k_{i-1}(M), ..., k_{i-N+1}(M)$.
  if the previous keys are authenticated **then**
    The reader is authenticated
  else if failed **then**
    The message will be considered forged and the authentication will failed.
    The tag would need to inform the reader and the reader would need to retransmit the updated key.
  end if
end if

Contribution

- For each authentication, the reader generates
  N MACs(message authentication codes

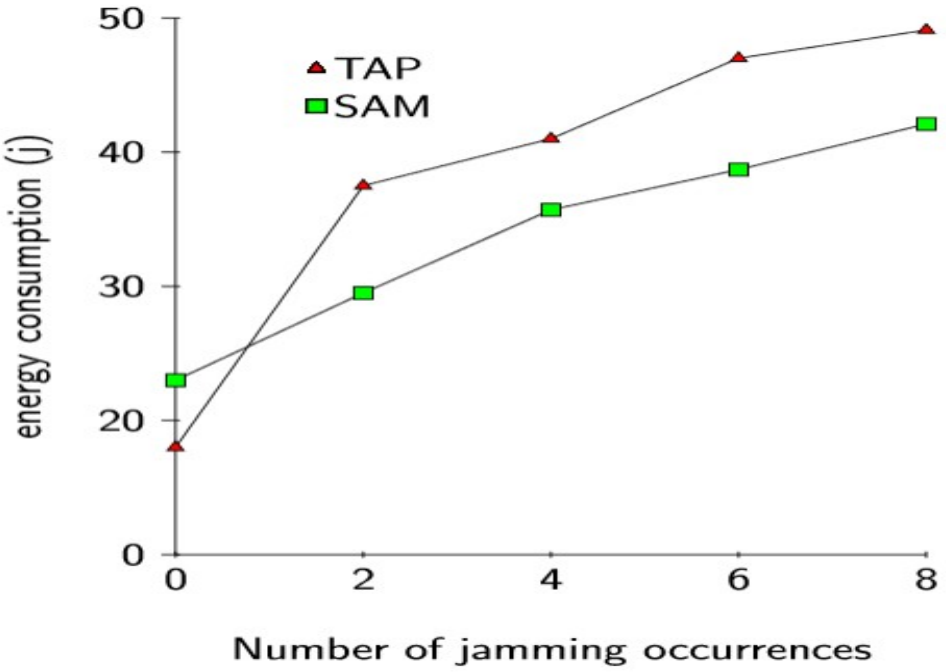
1

$S= <MAC(k_{updated,} M)|| MAC(k_{i,} M) || MAC(k_{i-1,} M)…., || MAC(k_{i-N+1,} M)>$

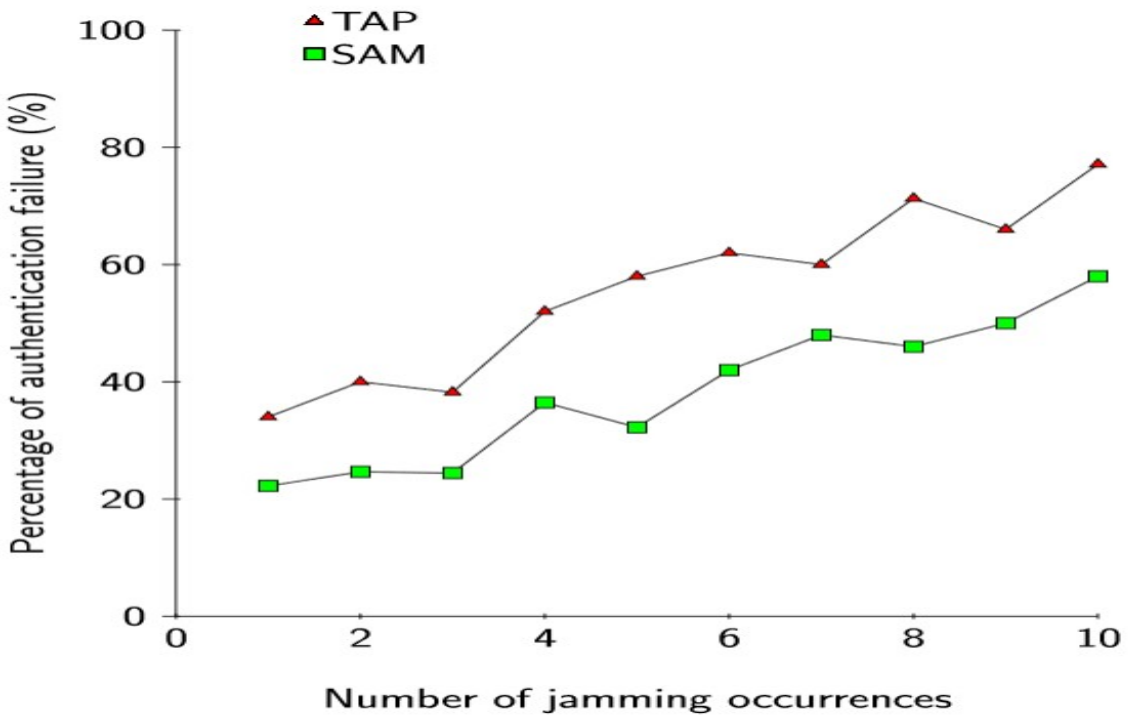
2

The readers have the property that if the updated keys are lost, they can be recomputed using previous keys,

Energy consumption



The average of authentication failure rate



Conclusion

- Radio Frequency Identification (RFID) is an exciting, rapidly growing, multidisciplinary technology, which is capable of automatically and uniquely identifying objects or persons by radio frequency within certain proximity.
- we have proposed a new self-adaptive RFID authentication protocol, named as SAM,
- One important advantage of our protocol is that it can be seamlessly deployed to existing systems for increasing the security of tag identification while at the same time maintaining the system efficiency.

Perspectives

RFID tags are likely to become even more popular in the future. Soon:

- As future work, we plan to deploy SAM for real-world IoT network and further consolidate the performance of proposed authentication algorithms.
- We will consider how to detect and discoverer other attacks against the RFID technology and will enhance its intrusion detection capabilities.

Questions and Discussion

Bacem Mbarek
Faculty of Informatics
Masaryk University
Brno, Czech Republic
bacem.mbarek@mail.muni.cz