An analysis of RFID authentication schemes with Secure Object Tracking Protocol for the Internet of Things.

Ms. Ashwini Bhore[1], Dr. Gayatri Bhandari[2]

Computer Engineering, JSPM'S Bhivrabai Sawant Institute of Technology & Research Wagholi, Pune-421207,Maharashtra,India

ABSTRACT

Most of the existing tracking protocol aims to increase the visibility of an object in a specific networked RFID system . A "path checker" object tracing and tracking protocol which stores state information to tag and uses key-based hash to perform the information exchange between the tag and the reader. This protocol uses many readers to authenticate and update a tag. Protocol assumes that tags are tamper resistant and capable of anticounterfeit mechanisms but which is invalid for RFID tags and thus it is only secure on a weak advisory model. Also, the path of an object can be checked at the end of the destination .So, we propose a secure object tracking protocol to ensure the visibility and traceability of an object along the travel path to support the Internet of Things (IoT). This protocol is based on radio frequency identification (RFID) system for global unique identification of IoT objects. To ensure secure object tracking, physically unclonable functions are used by the proposed protocol. Here, we modeled the protocol using security protocol description language (SPDL) and simulated SPDL model using automated claim verification tool Scyther. The results show that the proposed protocol is more secure and requires less computation compared to existing similar protocols.

Keyword : *Internet of Things (IoT), secure object tracking ,radio frequency identification (RFID).*

1. INTRODUCTION

Internet of Things (IoT) is the connection between devices, which can be uniquely identified through the IP addressing scheme and have the capability to communicate with other devices to attain the required objectives. IoT strives for providing the ability to interconnected devices in a network to transfer data without the need of human-human interaction or human-machine interaction. It aims to provide services directly based on machine-machine interaction. many important applications are provided by IoT, like Transportation,Logistics,Healthcare Smart environments ,Security applications. RFID is a very popular technology used for identification of objects automatically through Radio signals. The deployment of the RFID technology requires the following three components.

RFID Tag,
RFID Reader,
Backend Server/database

As radio frequency identification (RFID) does not require a line of sight to identify an object and can identify many objects at a time. An object in IoT may need to report to a number of partners before it reach to its owner or user . Hence, the objects in a global networked chain might travel between multiple business partners to fulfill business objectives. Later, the object might need to travel backwards from the user to the transporter and finally replacement or repair of supply chain.

The IoT system needs to verify the travel path and ensure on-site object tracking movement to ensure connectivity. It is also important to collect information on the status of the object along the path to improve forecasting accuracy, which helps to formulate strategies and reduce object transit time for users. However, in order to achieve these outcomes, the IoT system has to share and exchange information between objects and partners from a number of administrative domains via wireless media. A secure object tracking protocol ensure that an adversary should not compromise the privacy of the partners, the current owner (CO) or the objects while tracing and tracking things globally. It should also protect the tag from cloning and ensure the nonrepudiation. Although few protocols that address the tracking, tracing, and path verification of an object exist, they have either security vulnerabilities or not feasible to implement even in existing EPC active tags. In addition, existing tracking protocols did not clearly address nonrepudiation, injection of fake objects, and unclonability issues while tracking the object along the path. So, a secure tracking protocol to ensure the visibility and the traceability of an object along the path. This protocol also ensures the correctness of the travel-path while protecting the privacy of the CO, the partners, and the users.

2. RELATED WORK

The main aim of tracker protocol is to improve the visibility of the uniquely identifiable objects for legal owners. Most of the tracking protocol aims to maximize visibility of an object in a specific NRS, along the network. The object authenticity verification protocol validates the authenticity of an object along with its travel path. The proposal requires a centralized trusted party called a "manager" to carry out path verification. Bi and Lin [2]analysed the importance of finding the object along the path to minimize holding costs as well as accuracy. The path-checking solution and path-checking protocol [6] aim to combine authentication and path checking to ensure tracking and tracing of the tag in a supply chain. To make these proposals possible, all the partners in the network chain need to know the full path and store this information in the database.

3. IMPLEMENTATION DETAILS

3.1 Problem Statement

.In this paper, we study tracking of the tags on-site to ensure privacy, visibility, nonrepudiation, and protection from the injection of fake objects along the network chain.

3.2 Existing System

A secure object tracking protocol is an effective option available to verify authenticity as well as protect nonrepudation security property of system which is proposed to track and trace the tag along the path . The work of Bi and Lin[2] identified the importance of finding the object along the path for tracking and tracing to minimize inventory holding costs, improve forecasting accuracy,formulate strategies, and reduce transit time in supply chain. Ouafi and Vaudenay [3], proposed a "path checker" object tracing and tracking protocol which stores state information to the tag and uses key-based hash to perform the information exchange between the tag and the reader. Burbridge and Soppera [4] used a proxy resignature protocol to allow path segment verification while using read/write only tags, the tags store the signature of the last trusted party it has visited. Elkhiyaoui, Blass, and Molva [5] considered polynomial based encoding protocol that represent the path in a supply chain. Path validity can be checked in each partner by readers. Most of the existing tracking protocol aims to increase visibility of an object in a specific NRS (such as supply chain) using tracking and tracing along the network

3.2 Proposed System

The main objective of proposed system is to increase visibility of the unique identification for legal owners. Tracker protocol consists a set of tags that may travel between valid business partners in any order, this protocol performs a read, write securely to verify the authenticity and tracking of the tags on-site while ensuring privacy, protection from the injection of fake objects. The advantage of the adversary(A) is to regenerate legal response by interrogating the tag and is capable to monitor all wireless communications (between tags and partners) and gathering side channel information. And also capable of gathering some side channel information (except hardware based) The networked RFID system (NRS) perform object identification between widely distributed partners.

4. SYSTEM ARCHITECTURE

The system Architecture of proposed system is as shown in the figure Both the readers(Current owner(CO) and partner) execute a group of Deffie–Hellman algorithm to generate a shared secret key.They also exchange information to agree on a symmetric encryption algorithm that will be used in the protocol execution. Partners need to register themselves to CO using their unique PID to become a semi-trusted partner. Let PIDi be the unique ID of partner Pi and RIDCO be the unique identification of the CO reader Each registered partner (P) receives a tuple below from CO to securely execute the tracker protocol . The system calculates a common challenge value (c) by performing hash operation on XORed value of the PC and CO reader's ID. The tagged objects can travel to a partner (Pi ∈ P) in. The tag has a PUF() function to support the required cryptographic operations. There is a secret key shared between CO and the tag (Ti). The backend of the CO stores the tuple COTi for each tag.

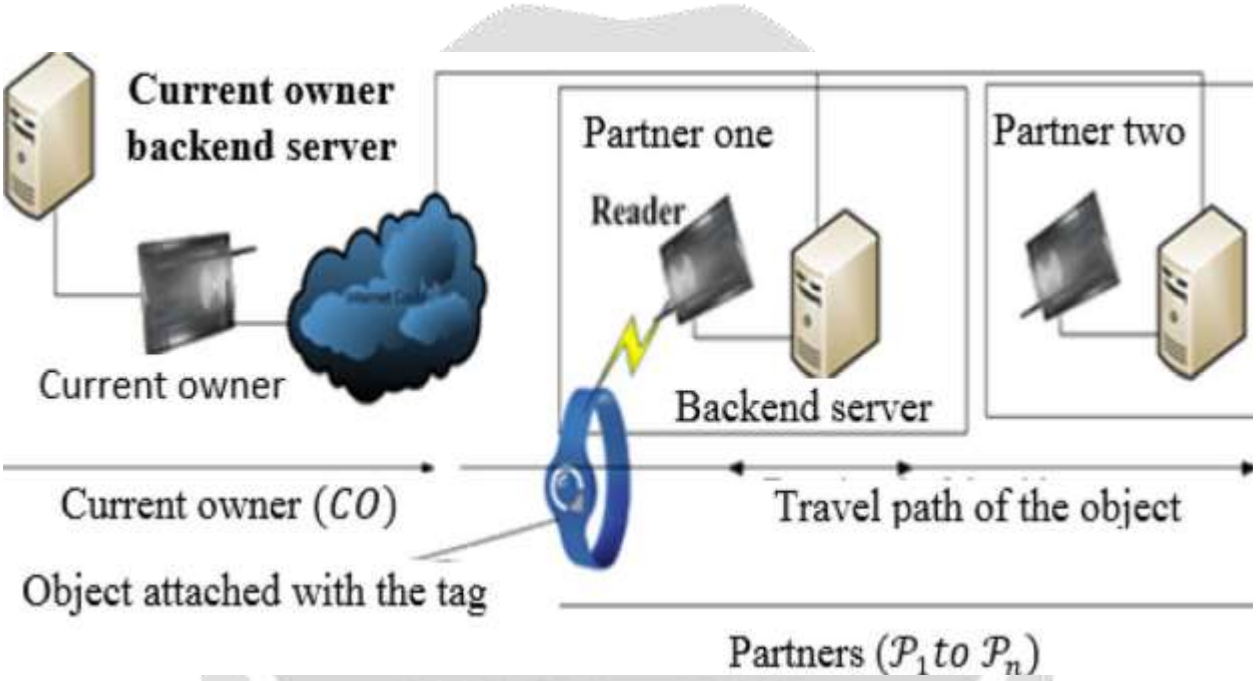

Fig. System Architecture

5. MODULE DISCRIPTION

In this section we present the Module description, how it works, practical results and environment.

Current Owner(co): CO owns a tag that travels to a number of partners to achieve a business objective and also keeps track of the tag along the travel path via partner readers. Each registered partner (P) receives a tuple below from CO to securely execute tracker protocol.

Partner: The partners have a shared secure communication link with the CO over a cloud using conventional secure communication techniques such as IPSec. In addition, the partners are semitrusted. The tagged objects can travel to a partner (Pi ∈ P) in any order but can only travel once in a specific journey. It also lets CO track the tag and verify the travel path of the tag while protecting the required security of the system and users.

Backend server: The backend of the CO stores the tuple for each tag and a tuple for the path a tag may travel is the secret key shared between CO and the tag. The tag's travel status is updated in both the tag and in the CO's backend.

Object attached with tag: The tag itself is the only one who can write on this protected user memory. Initially, all the bits in the protected memory are represented by "OFF" = 0 bit. After successful mutual verification of the travel status between the CO, partners and the tag, the tag will set a bit "ON" = 1 in a certain position. The position value is determined by the ith value of the partner so that po = i.

6. RESULT

In this section, we compare our protocol with existing similar protocols based on cryptographic requirements and performance.

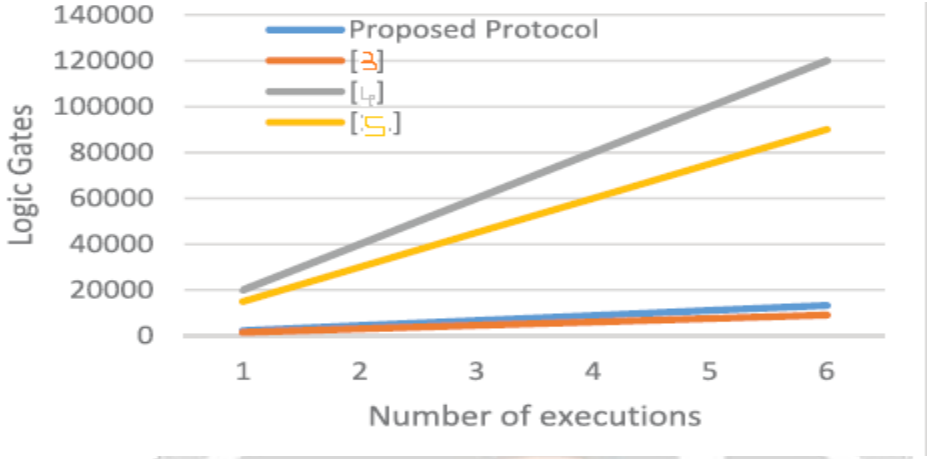

Fig. Comparison between performance of protocol

Regarding performance of a cryptographic protocol, our proposed protocol performs better than protocol [3], [4]. Protocol [5] has better performance than our proposed protocol but it violates many required security properties for a tracker protocol. Fig. shows performance comparison between our proposed protocol and some similar requirements.

7. CONCLUSION

Focusing on the the issue of traceability and visibility of the object throughout the chain, the protocol has to ensure security such as privacy. The proposed secure tracker protocol increase an object's tracking and tracing to enhance the visibility of objects and ensures nonrepudiation along with privacy of the NRS. It uses the PUF function for preventing injection of fake tag into the chain. The protocol is computationally feasible to implement low cost RFID tags as well as application independent. Furthermore needs to develop a generalized protocol that can collect the relevant context information of an object to ensure context awareness. This will increase control over an object to improve development of the IoT.

REFERENCES

[1]. Biplob R. Ray, Member, IEEE, Morshed U. Chowdhury, Member, IEEE, and Jemal H. Abawajy, Senior Member, IEEE.
[2]. T. Burbridge and A. Soppera, "Supply chain control using a RFID proxy re-signature scheme," in Proc. IEEE Int. Conf. RFID, Orlando, FL, USA,2010, pp. 29–36.
[3]. K. Ouafi and S. Vaudenay, "Pathchecker: An RFID application for tracing products in suply-chains," in Proc. Inf. Security Group (GSI), Leuven, Belgium, 2009, pp. 1–14.
[4]. H. H. Bi and D. K. J. Lin, "RFID-enabled discovery of supply networks," IEEE Trans. Eng. Manage., vol. 56, no. 1, pp. 129–141, Feb. 2009.
[5]. K. Elkhiyaoui, E.-O. Blass, and R. Molva, "CHECKER: On-site checking in RFID-based supply chains," in Proc. 5th ACM Conf. Security Privacy Wireless Mobile Netw., Tucson, AZ, USA, 2012,pp. 173–184.
[6]. W. Xin, H. Sun, T. Yang, Z. Guan, and Z. Chen, "A privacy-preserving path-checking solution for RFID-based supply chains," in Information and Communications Security, vol. 7618, T. Chim and T. Yuen, Eds. Heidelberg, Germany: Springer, 2012, pp. 400–407.