Received May 15, 2020, accepted June 28, 2020, date of publication July 7, 2020, date of current version July 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3007771

A New Strong Adversary Model for RFID Authentication Protocols

MEHDI HOSSEINZADEH[1,2], JAN LANSKY[3], AMIR MASOUD RAHMANI[4], CUONG TRINH[5], MASOUMEH SAFKHANI[6], NASOUR BAGHERI[7,8], AND BAO HUYNH[9]

[1] Institute of Research and Development, Duy Tan University, Da Nang 550000, Vietnam
[2] Health Management and Economics Research Center, Iran University of Medical Sciences, Tehran 14496-14535, Iran
[3] Department of Computer Science and Mathematics, Faculty of Economic Studies, University of Finance and Administration, Prague 101 00, Czech Republic
[4] Department of Computer Science, Khazar University, Baku 1009, Azerbaijan
[5] Artificial Intelligence Laboratory, Faculty of Information Technology, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
[6] Computer Engineering Department, Shahid Rajaee Teacher Training University, Tehran 16788-15811, Iran
[7] Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran 16788-15811, Iran
[8] School of Computer Science (SCS), Institute for Research in Fundamental Sciences (IPM), Farmanieh Campus, Tehran 19538 33511, Iran
[9] Faculty of Information Technology, Ho Chi Minh City University of Technology (HUTECH), Ho Chi Minh City 700000, Vietnam

Corresponding author: Bao Huynh (hq.bao@hutech.edu.vn)

This work was supported by using the institutional support for a long-term conceptual development of research organization University of Finance and Administration.

ABSTRACT Radio Frequency Identification (RFID) systems represent a key technology for ubiquitous computing and for the deployment of the Internet of Things (IoT). In RFID technology, authentication protocols are often necessary in order to confirm the identity of the parties involved (i.e. RFID readers, RFID tags and/or database servers). In this article, we analyze the security of a mutual authentication protocol proposed by Wang and Ma. Our security analysis clearly shows major security pitfalls in this protocol. Firstly, we show two approaches that an adversary may use to mislead an honest reader into thinking that it is communicating with a legitimate database. Secondly, we show how an adversary that has compromised some tags can impersonate an RFID reader to a legitimate database. Furthermore, we present a new adversary model, which pays heed on cases missed by previous proposals. In contrast to previous models where the communication between an RFID reader and a back-end server is through a secure channel, our model facilitates the security analysis of more general schemes where this communication channel (RFID reader-to-server) is insecure. This model determines whether the compromise of RFID tags has any impact on the security of the reader-to-server communication or vice versa. In a secure protocol, the possible compromise of RFID tags should not affect the RFID reader-server communication. In this paper, we show that compromising of RFID tags in Wang and Ma protocol has a direct impact on the reader-server security. Finally, we propose a new authentication protocol that offers an adequate security level and is resistant against the mentioned security risks. The security proofs of the proposed protocol are supported with Gong-Needham-Yahalom (GNY) logic and Scyther tool, which are formal methods to evaluate the security of a cryptographic protocol.

INDEX TERMS Adversary model, IoT, RFID, authentication, security analysis, scyther tool, GNY logic.

I. INTRODUCTION

The Internet of Things (IoT) envisions applications where multiple objects interact and cooperate, provide different services and are accessible at any time from many points [1], [2]. More precisely, given many available features such as social networks, software defined optical networks (SDONs), fifth generation (5G) cellular networks, Internet of Vehicles (IoV), Internet of Energy (IoE), Internet of Sensors (IoS), Machine to Machine Communications (M2M), artificial intelligence and machine and deep learning this vision will advance more, although it will also cope with new challenges as well [3]. Among those features, 5G cellular networks provide key enabling technologies for ubiquitous deployment of the IoT technology, that are include multiple-input multiple-output (MIMO), massive-MIMO (M-MIMO), coordinated multipoint processing (CoMP), device-to-device (D2D) communications, centralized radio access network (CRAN), software-defined wireless sensor networking (SD-WSN), network function virtualization (NFV) and cognitive

The associate editor coordinating the review of this manuscript and approving it for publication was Wen Chen.

radios (CRs) [4]. Hence, a widely accepted vision of IoT is that any object can become a computing device that interacts autonomously, in real-time, with its environment. With the worldwide number of connected devices that are expected to increase from nearly 27 billion connected devices in 2017 to 125 billion connected devices by 2030 [5], [6], that vision will become a reality very soon. On the other hand, based on an study from Business Fortune Insights (BFI) the global IoT market, that valued at US$ 190 billion in 2018, is expected to reach US$ 1,102.6 billion by 2026 [7].

Although the connectivity of devices increases significantly, but advances in IoT architectures, protocols and adversary models are still necessary to make the vision of the IoT reality. Among all the technologies immersed in IoT, Radio Frequency Identification (RFID) technology is one of the most prominent due to its maturity, low cost and strong support from the industry [8].

RFID components include a tag (including a semiconductor chip, an antenna and sometimes a battery), a reader (including an antenna, an RF electronic module and a control module) and a back-end (database) server (for example, a computer device that has a database and control software runs on it). The exchange of information between the RFID tag and the reader is done using radio waves. Reader's connection to the back-end (database) server is either permanent through a secure channel or non-permanent through an unsafe channel.

In RFID systems, to achieve one-end or mutual authentication, readers and tags may employ authentication protocols (e.g. [9]–[13]). Despite recent advances in the domain of RFID communication, the design of secure authentication protocols has remained as a challenge yet [14], given the constraints of those devices, e.g. available power. For example, several researches tried to provide desired security for RFID system only using ultralightweigh operations, such as bitwise XOR, AND and rotation. However, later analysis have shown that it may not be possible to design a secure protocol without using sound cryptographic primetives [15], [16].

RFID authentication protocols can be divided into two broad categories: (i) those with a permanent connection to a back-end (database) server and (ii) those without a permanent connection to a back-end (database) server (i.e. *server-less* authentication protocols). Most of the existing RFID authentication protocols belong in the first category (i.e. they use a back-end server in their authentication process). In a *back-end server based* authentication protocol, the reader communicates with the back-end server to obtain all the data linked to the target tag through a secure channel i.e. a reliable and permanent connection between the RFID reader and the back-end server. However, in some applications and scenarios it may be impossible to provide a connection between the RFID reader and the back-end server, e.g. any application that may need a mobile RFID reader without or with very limited connectivity. For instance, a ticket inspector at trains is armed with an RFID reader which has a wireless connection with a back-end (database) server through a non-secure channel. Another example is the telecare medicine where the nurse should use a mobile reader and it is not reasonable to assume that the reader has a permanent connection with the server [17].

Therefore, to cover such scenarios, several server-less authentication protocols have been proposed in the literature [18]–[24]. However, when two parties are communicating over a public channel then the adversary could affect the transferred messages, for example to do a Man-in-the-Middle Attack [25], this is the case for the server-reader communication also. In this direction, Wang and Ma [20] have analyzed the security of a *server-less mutual authentication* protocol, which has been proposed by Tan *et al.* [19], and showed that this protocol is vulnerable to tracing attacks. Moreover, they proposed two improved protocols, denoted by server-less and server-mounted respectively, and claimed that the new protocols are secure against all the common attacks on the RFID context, i.e. eavesdropping, replay, impersonation and DoS attacks. However, recently Gao *et al.* have shown that the server-less protocol suffers from traceability attack [26]. In this article, we also show that the major security pitfalls of server-mounted authentication protocol, we call it SMAP (stands for server-mounted authentication protocol), which has been proposed by Wang and Ma [20].

Our Contribution: Our main contributions are three-fold:

1) We analyze the security of a server-mounted mutual authentication protocol which has been proposed by Wang and Ma [20] and highlight its weaknesses. Our security analysis clearly highlights critical security pitfalls in this protocol. This work completes the recent work of Gao *et al.* [26].
2) We introduce a novel security model which can be employed in order to analyze the security of a protocol for which the communication channel between a reader and the back-end server is insecure. In this model, we assume that an adversary $\mathcal{A}$ has already compromised some tags. We investigate what is the impact of this assumption on the security of the *reader-to-server communication channel* and vice versa. In addition, we scrutinize the security of the above mentioned protocol i.e. SMAP [20] using this model and show that in this model the scheme is vulnerable.
3) Finally, we provide some countermeasures that can be employed to overcome the exhibited flaws and provide an improved protocol, called ISMAP (stands for improved server-mounted authentication protocol), which is secure under the new security model. In Addition, using supported GNY logic and the Scyther tool, we formally evaluate the proposed protocol's security.

Organization: The paper is organized as following. Section II describes the Wang and Ma authentication protocol [20]. In Section III, the security analysis of this protocol is presented. Section IV introduces the new security model and our analysis of the Wang and Ma authentication protocol [20] using this model. In Section V, we describe some

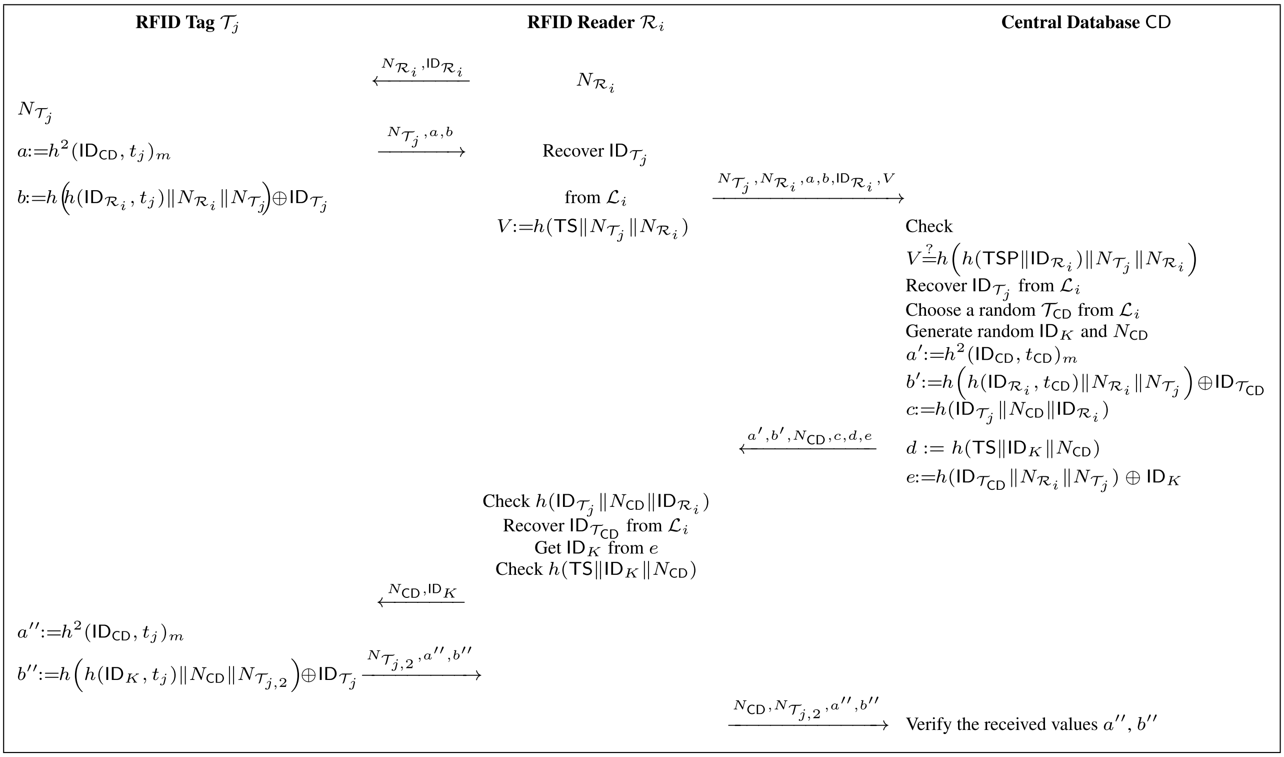

RFID Tag $\mathcal{T}_j$
RFID Reader $\mathcal{R}_i$
Central Database CD
$\xleftarrow{N_{\mathcal{R}_i}, \mathsf{ID}_{\mathcal{R}_i}}$
$N_{\mathcal{R}_i}$
$N_{\mathcal{T}_j}$
$a{:=}h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m$
$\xrightarrow{N_{\mathcal{T}_j}, a, b}$
Recover $\mathsf{ID}_{\mathcal{T}_j}$
$b{:=}h\Big(h(\mathsf{ID}_{\mathcal{R}_i}, t_j)\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j}\Big)\oplus\mathsf{ID}_{\mathcal{T}_j}$
from $\mathcal{L}_i$
$\xrightarrow{N_{\mathcal{T}_j}, N_{\mathcal{R}_i}, a, b, \mathsf{ID}_{\mathcal{R}_i}, V}$
$V{:=}h(\mathsf{TS}\|N_{\mathcal{T}_j}\|N_{\mathcal{R}_i})$
Check
$V \overset{?}{=} h\Big(h(\mathsf{TSP}\|\mathsf{ID}_{\mathcal{R}_i})\|N_{\mathcal{T}_j}\|N_{\mathcal{R}_i}\Big)$
Recover $\mathsf{ID}_{\mathcal{T}_j}$ from $\mathcal{L}_i$
Choose a random $\mathcal{T}_{\mathsf{CD}}$ from $\mathcal{L}_i$
Generate random ID_K and N_{CD}
$a'{:=}h^2(\mathsf{ID}_{\mathsf{CD}}, t_{\mathsf{CD}})_m$
$b'{:=}h\Big(h(\mathsf{ID}_{\mathcal{R}_i}, t_{\mathsf{CD}})\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j}\Big)\oplus\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}}$
$c{:=}h(\mathsf{ID}_{\mathcal{T}_j}\|N_{\mathsf{CD}}\|\mathsf{ID}_{\mathcal{R}_i})$
$\xleftarrow{a', b', N_{\mathsf{CD}}, c, d, e}$
$d := h(\mathsf{TS}\|\mathsf{ID}_K\|N_{\mathsf{CD}})$
$e{:=}h(\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}}\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j}) \oplus \mathsf{ID}_K$
Check $h(\mathsf{ID}_{\mathcal{T}_j}\|N_{\mathsf{CD}}\|\mathsf{ID}_{\mathcal{R}_i})$
Recover $\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}}$ from $\mathcal{L}_i$
Get ID_K from e
Check $h(\mathsf{TS}\|\mathsf{ID}_K\|N_{\mathsf{CD}})$
$\xleftarrow{N_{\mathsf{CD}}, \mathsf{ID}_K}$
$a''{:=}h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m$
$b''{:=}h\Big(h(\mathsf{ID}_K, t_j)\|N_{\mathsf{CD}}\|N_{\mathcal{T}_{j,2}}\Big)\oplus\mathsf{ID}_{\mathcal{T}_j}$
$\xrightarrow{N_{\mathcal{T}_{j,2}}, a'', b''}$
$\xrightarrow{N_{\mathsf{CD}}, N_{\mathcal{T}_{j,2}}, a'', b''}$
Verify the received values a'', b''

FIGURE 1. SMAP: the server-mounted authentication protocol proposed by Wang and Ma.

countermeasures that can be employed to overcome the described weaknesses. Finally, Section VI concludes the paper.

II. WANG AND MA SERVER-MOUNTED MUTUAL AUTHENTICATION PROTOCOL DESCRIPTION

Wang and Ma [20] have analyzed the security of the *server-less mutual authentication* protocol proposed by Tan *et al.* [19] and have shown that this protocol is vulnerable to tracing attacks. To overcome these attacks, Wang and Ma [20] proposed two new protocols, a server-less protocol and a server-mounted protocol. Recently Gao *et al.* have analysed the server-less protocol in depth and the target of this paper is the server-mounted protocol, which is called SMAP for the sake of simplicity. Fig. 1 depicts this protocol, while Table 1 represents the notations that are used in the rest of the paper. SMAP includes four entities:

- an RFID tag ($\mathcal{T}_j$) with a unique identifier $\mathsf{ID}_{\mathcal{T}_j}$ and a unique secret key t_j,

- an RFID reader ($\mathcal{R}_i$) with unique identifier $\mathsf{ID}_{\mathcal{R}_i}$, - a certification authority (CA),

- and a central database (CD) server with a unique identifier $\mathsf{ID}_{\mathsf{CD}}$.

Furthermore, both the RFID tag ($\mathcal{T}_j$) and the RFID reader ($\mathcal{R}_i$) use a hash function $h(\cdot)$, which could be a lightweight hash function such as PHOTON [27] or Quark [28]. Wang and Ma [20] protocol can be divided into four phases: the *setup* phase, the *server-less authentication* phase, the *tag authentication* phase and the *tag searching* phase.

A. SETUP PHASE

In this phase, each RFID reader ($\mathcal{R}_i$) after being authenticated to the Certification Authority (CA) receives: i) its unique identifier $\mathsf{ID}_{\mathcal{R}_i}$, ii) a *timestamp* $\mathsf{TS} = h(\mathsf{TSP}\|\mathsf{ID}_{\mathcal{R}_i})$[1] where TSP is a time dependent value of the central database (CD) which is updated periodically and, iii) an access list $\mathcal{L}_i$ for the tags $\mathcal{T}_1, \ldots, \mathcal{T}_n$ such that:

$$\mathcal{L}_i = \Big\{\Big(h(\mathsf{ID}_{\mathsf{CD}}, t_1)_m, h(\mathsf{ID}_{\mathcal{R}_i}, t_1), \mathsf{ID}_{\mathcal{T}_1}\Big), \ldots, \Big(h(\mathsf{ID}_{\mathsf{CD}}, t_n)_m, h(\mathsf{ID}_{\mathcal{R}_i}, t_n), \mathsf{ID}_{\mathcal{T}_n}\Big)\Big\},$$

where m denotes the number of bits defined by the certification authority (CA) and ℓ is the output length of the hash function $h(\cdot)$. It holds that $m < \ell$.

B. SERVER-LESS AUTHENTICATION PHASE

This phase is composed of three steps:

- **Step 1:** The RFID reader ($\mathcal{R}_i$) sends its identifier $\mathsf{ID}_{\mathcal{R}_i}$ and a random number $N_{\mathcal{R}_i}$ to the RFID tag $\mathcal{T}_j$.
- **Step 2:** The RFID tag ($\mathcal{T}_j$) transmits to the RFID reader ($\mathcal{R}_i$) its random number $N_{\mathcal{T}_j}$ and the values a and b such that:

$$a := h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m$$
$$b := h\Big(h(\mathsf{ID}_{\mathcal{R}_i}, t_j)\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j}\Big) \oplus \mathsf{ID}_{\mathcal{T}_j}$$

- **Step 3:** The RFID reader ($\mathcal{R}_i$) checks its access list $\mathcal{L}_i$ and compares the first part of each entry in the list

[1] TS which can be used as an identification value for the RFID reader $\mathcal{R}_i$.

TABLE 1. Notations.

Notation	Description
$\mathcal{R}_i$	the RFID reader i
$\mathsf{ID}_{\mathcal{R}_i}$	the static identifier of $\mathcal{R}_i$
$\mathcal{T}_j$	the RFID tag j
$\mathsf{ID}_{\mathcal{T}_j}$	the static identifier of the RFID tag $\mathcal{T}_j$
t_j	the secret key of the RFID tag $\mathcal{T}_j$
CD	the central database server
$\mathsf{ID}_{\mathsf{CD}}$	the static identifier of CD
$N_{\mathcal{R}_i}$	a random number generated by $\mathcal{R}_i$
$N_{\mathcal{T}_j}$	a random number generated by $\mathcal{T}_j$
$\mathcal{L}_i$	the access list for $\mathcal{R}_i$
n	number of entries in the access list $\mathcal{L}_i$
$h(\cdot)$	the one-way hash function
$h(x, y)$	$h(x\|y)$
$h^2(\mathcal{X})$	$h(h(\mathcal{X}))$
CA	a certification authority, trusted party responsible for authenticating RFID readers and deploying tags
$\mathcal{X}^i$	the value of parameter $\mathcal{X}$ on session i
ℓ:	output length of the hash function $h(.)$
m	number of bits defined by CA, $m < \ell$
TSP	the time stamp of CD
TS	the time stamp of the RFID reader, $TS = h(\mathsf{TSP}\|\mathsf{ID}_{\mathcal{R}_i})$
ID_K	a temporal RFID reader identifier for implicit authentication between the RFID reader and the CD which is generated by the CD in the authentication phase
$A \to B$	sending a message from A to B
$\oplus$	Exclusive or operation
$\|$	Concatenation operation
$A \to B$	sending a message from A to B

with the received value a listing all matched entries. For each matched entry, the RFID reader ($\mathcal{R}_i$) computes the values $h\Big(h(\mathsf{ID}_{\mathcal{R}_i}, t_j)\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j}\Big) \oplus \mathsf{ID}_{\mathcal{T}_j}$ and compares them with the received value b. The case that no match is found in, implies that either the requested tag $\mathcal{T}_j$ is fake or that the RFID reader $\mathcal{R}_i$ is not authorized to read the tag $\mathcal{T}_j$.

C. SERVER-MOUNTED AUTHENTICATION PHASE

This phase can be divided into five following steps:

- **Step 1:** The RFID reader ($\mathcal{R}_i$) has identified the RFID tag ($\mathcal{T}_j$) with identity $\mathsf{ID}_{\mathcal{T}_j}$. Then the RFID reader ($\mathcal{R}_i$) sends the tuple $(N_{\mathcal{R}_i}, N_{\mathcal{T}_j}, a, b, \mathsf{ID}_{\mathcal{R}_i}, V)$ where
  $V := h(\mathsf{TS}\|N_{\mathcal{T}_j}\|N_{\mathcal{R}_i})$ to the central database (CD).
- **Step 2:** The central database (CD) receives the tuple sent by the RFID reader ($\mathcal{R}_i$) and verifies the correctness of the received value V. In case the received value V is not verified, the whole protocol aborts. If the value V is verified then the central database (CD) using the access list $\mathcal{L}_i$ and the value a finds the tag's ($\mathcal{T}_j$) record and the related $\mathsf{ID}_{\mathcal{T}_j}$. Then, the central database (CD) chooses a random tag $\mathcal{T}_{\mathsf{CD}}$ from the access list $\mathcal{L}_i$ (of the current reader $\mathcal{R}_i$) with identifier $\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}}$ and secret t_{CD}. CD also chooses a random identifier ID_K and a random nonce N_{CD} and calculates the below messages:
  $$\begin{aligned} a' &:= h^2(\mathsf{ID}_{\mathsf{CD}}, t_{\mathsf{CD}})_m \\ b' &:= h\Big(h(\mathsf{ID}_{\mathcal{R}_i}, t_{\mathsf{CD}})\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j}\Big) \oplus \mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}} \\ c &:= h(\mathsf{ID}_{\mathcal{T}_j}\|N_{\mathsf{CD}}\|\mathsf{ID}_{\mathcal{R}_i}) \\ d &:= h(\mathsf{TS}\|\mathsf{ID}_K\|N_{\mathsf{CD}}) \\ e &:= h(\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}}\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j}) \oplus \mathsf{ID}_K \end{aligned}$$
  Then, CD sends the tuple $(a', b', N_{\mathsf{CD}}, c, d, e)$ back to the RFID reader ($\mathcal{R}_i$).
- **Step 3:** The RFID reader ($\mathcal{R}_i$) verifies the correctness of the received value $c := h(\mathsf{ID}_{\mathcal{T}_j}\|N_{\mathsf{CD}}\|\mathsf{ID}_{\mathcal{R}_i})$. Then, $\mathcal{R}_i$ finds the record of $\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}}$ in its memory, based on the received information from CD. It extracts $\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}}$, calculates ID_K from the value of $e := h(\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}}\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j}) \oplus \mathsf{ID}_K$ and verifies the correctness of the received value $d := h(\mathsf{TS}\|\mathsf{ID}_K\|N_{\mathsf{CD}})$ to authenticate CD. Then the RFID reader ($\mathcal{R}_i$) sends N_{CD} and ID_K to the RFID tag $\mathcal{T}_j$.
- **Step 4:** The RFID tag ($\mathcal{T}_j$) generates a new random nonce $N_{\mathcal{T}_{j,2}}$ and sends to the central database (CD) the tuple:
  $$\Big\{N_{\mathcal{T}_{j,2}}, h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m, \\ h\Big(f(\mathsf{ID}_K, t_j)\|N_{\mathsf{CD}}\|N_{\mathcal{T}_{j,2}}\Big) \oplus \mathsf{ID}_{\mathcal{T}_j}\Big\}$$
- **Step 5:** The central database (CD) receives the above mentioned tuple and verifies the correctness of the values $h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m$ and $h\Big(f(\mathsf{ID}_K, t_j)\|N_{\mathsf{CD}}\|N_{\mathcal{T}_{j,2}}\Big)$. If these values are correct then the RFID reader ($\mathcal{R}_i$) is authenticated to access the RFID tag $\mathcal{T}_j$ and further information is transferred.

D. TAG SEARCHING PHASE

The RFID tag searching scheme can be built by using the server-less authentication scheme. The RFID reader starts broadcasting its identifier $\mathsf{ID}_{\mathcal{R}_i}$ and a random number $N_{\mathcal{R}_i}$ to an RFID tag population. The RFID tags in the RFID reader's range will respond with $N_{\mathcal{T}_j}$, a and b (i.e., $a := h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m, b := h\Big(h(\mathsf{ID}_{\mathcal{R}_i}, t_j)\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j}\Big) \oplus \mathsf{ID}_{\mathcal{R}_i}$). The RFID reader knows in advance the tag identifier $\mathsf{ID}_{\mathcal{T}_j}$ and the corresponding a of the target RFID tag. So, it filters all the responses with a different a and with the desired answer, it checks b and identifies the pursued RFID tag.

III. SECURITY ANALYSIS OF SMAP

In this section, we analyze the security of the Wang and Ma [20] *server-mounted authentication protocol (SMAP)* and highlight its critical weaknesses. Before we describe the identified weaknesses, we should note here the classification of information in the RFID communication according to the Wang and Ma [20] protocol. More precisely, in [20] information depending on the confidentiality level be fall into following levels:

Level 1: In this level, the least confidential information are included in RFID tags. More precisely, information such as the RFID tags' identifiers or other basic information such as the destination of attached goods are stored on the RFID tags.

Level 2: In this level, more privileged information such as the source of the tagged goods or the expected delivery date are included in the RFID readers.

Level 3: In this level, more confidential information such as the type of the tagged goods and their owner are stored by the central database (CD) and they are accessible only to the authenticated RFID readers. The central database (CD) also keeps other lower-level information and the registration information of the readers.

In the rest of this section, we describe in details the flaws we have identified in the *server-mounted authentication protocol (SMAP)* proposed by Wang and Ma [20]. The first weakness allows an active adversary ($\mathcal{A}$) who has already compromised an RFID tag $\mathcal{T}_j \in \mathcal{L}_i$, to impersonate the central database (CD) server and the RFID tag ($\mathcal{T}_j$) to the RFID reader ($\mathcal{R}_i$). The second weakness allows an active adversary ($\mathcal{A}$), who has compromised some RFID tags, to impersonate the RFID reader ($\mathcal{R}_i$) to the central database (CD) server and receive the level-3 information for the compromised RFID tag from the central database server (CD).

A. CENTRAL DATABASE IMPERSONATION ATTACK

Following the given classification of information in the SMAP, the central database (CD) server keeps both low-level information and the most valuable information of the system. Hence, impersonating the central database (CD) server can have the most serious impact on the protocol functionality, since an adversary ($\mathcal{A}$) that successfully impersonates the CD can transfer wrong information (i.e. information belonging in level-3 according to the Wang and Ma classification). On the other hand, to authenticate the CD, the following conditions should hold:

1) The RFID reader ($\mathcal{R}_i$) should verify the correctness of the received value $h(\mathsf{ID}_{\mathcal{T}_j} \| N_{\mathsf{CD}} \| \mathsf{ID}_{\mathcal{R}_i})$.
2) $\mathcal{R}_i$ should find the record of $\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}}$ in its memory, based on the received information from the CD. In this way, $\mathcal{R}_i$ may extract the identifier $\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}}$.
3) R_i should calculate the identifier ID_K from the value of $e := h(\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}} \| N_{\mathcal{R}_i} \| N_{\mathcal{T}_j}) \oplus \mathsf{ID}_K$ and verifies the correctness of the received value $d := h(\mathsf{TS} \| \mathsf{ID}_K \| N_{\mathsf{CD}})$ to authenticate the CD.

Nevertheless, we present two scenarios that may be used by an adversary $\mathcal{A}$ in order to impersonate the central database (CD) server to the RFID reader ($\mathcal{R}_i$). In the first scenario, we show that an active adversary $\mathcal{A}$ which controls the communication channel between the CD and $\mathcal{R}_i$ can pass two out of the above described conditions easily. Then, we present another scenario, in which an active adversary $\mathcal{A}$ who has compromised an RFID tag $\mathcal{T}_j$ belonging in the access list $\mathcal{L}_i$ can pass all three conditions.

In the first scenario, to pass the first two conditions, the adversary ($\mathcal{A}$) does as follows:

Learning Phase: In this phase of the attack, the adversary ($\mathcal{A}$) eavesdrops one session of the authentication phase of a protocol run between the RFID reader ($\mathcal{R}_i$) (connected to the RFID tag ($\mathcal{T}_j$)) and the central database (CD) server but blocks the last messages from the CD to the $\mathcal{R}_i$. It also stores $h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m, h(\mathsf{TS} \| \mathsf{ID}_K \| N_{\mathsf{CD}}),\ h(\mathsf{ID}_{\mathcal{T}_j} \| N_{\mathsf{CD}} \| \mathsf{ID}_{\mathcal{R}_i})$ and N_{CD} that are transferred from CD to $\mathcal{R}_i$ over an insecure wireless channel that is easily accessible by the adversary $\mathcal{A}$.

CD Impersonation Phase: In this phase of the attack, in order to impersonate the target CD the adversary $\mathcal{A}$ does as follows:

- Step 1: When the RFID reader ($\mathcal{R}_i$) (connected to $\mathcal{T}_j$) sends the tuple $(N'_{\mathcal{R}_i}, N'_{\mathcal{T}_j}, a, b, \mathsf{ID}_{\mathcal{R}_i}, V)$ where

$$\begin{aligned} a &:= h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m \\ b &:= h\Big(h(\mathsf{ID}_{\mathcal{R}_i}, t_j) \| N'_{\mathcal{R}_i} \| N'_{\mathcal{T}_j}\Big) \oplus \mathsf{ID}_{\mathcal{T}_j} \\ V &:= h(\mathsf{TS} \| N_{\mathcal{T}_j} \| N_{\mathcal{R}_i}) \end{aligned}$$

to the CD server, the adversary ($\mathcal{A}$) selects the following values:

$$\begin{aligned} a' &:= h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m \\ b' &:= h\Big(h(\mathsf{ID}_{\mathcal{R}_i}, t_j) \| N'_{\mathcal{R}_i} \| N'_{\mathcal{T}_j}\Big) \oplus \mathsf{ID}_{\mathcal{T}_j} \\ c &:= h(\mathsf{ID}_{\mathcal{T}_j} \| N_{\mathsf{CD}} \| \mathsf{ID}_{\mathcal{R}_i}) \\ d &:= h(\mathsf{TS} \| \mathsf{ID}_K \| N_{\mathsf{CD}}) \\ e &:= h(\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}} \| N_{\mathcal{R}_i} \| N_{\mathcal{T}_j}) \oplus \mathsf{ID}_K \end{aligned}$$

and sends the tuple $(a', b', N_{\mathsf{CD}}, c, d, e)$ back to the RFID reader ($\mathcal{R}_i$).

- Step 2: The RFID reader ($\mathcal{R}_i$) verifies the correctness of the received value $d := h(\mathsf{ID}_{\mathcal{T}_j} \| N_{\mathsf{CD}} \| \mathsf{ID}_{\mathcal{R}_i})$. Then, $\mathcal{R}_i$ finds the record of $\mathsf{ID}_{\mathcal{T}_j}$ as $\mathcal{T}_{CD}$ in its memory and extracts $\mathsf{ID}_{\mathcal{T}_j}$ as $\mathsf{ID}_{\mathcal{T}_{CD}}$, calculates ID_K from the value of $e := h(\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}} \| N_{\mathcal{R}_i} \| N_{\mathcal{T}_j}) \oplus \mathsf{ID}_K$ and verifies the correctness of the received value $d := h(\mathsf{TS} \| \mathsf{ID}_K \| N_{\mathsf{CD}})$ to authenticate CD.

Hence, following the given procedure, the adversary ($\mathcal{A}$) passes two of the required three conditions to be authenticated as the legitimate central database (CD) server with the success probability equal to 1. However, the adversary ($\mathcal{A}$) can pass the last condition with probability $\frac{1}{2^\ell}$, where ℓ is the output length of the hash function. Although the above adversary has a negligible chance to pass the last condition, the observation that two conditions can be easily bypassed indicates a weak point in the design of Wang and Ma protocol [20].

Now, we present another *impersonation* attack which is based on the assumption that the adversary has already compromised a tag $\mathcal{T}_j \in \mathcal{L}_i$. To impersonate the central database

(CD) server in this scenario, the adversary ($\mathcal{A}$) does as follows:

Learning Phase:

- Step 1: Assume that $\mathcal{A}$ has already compromised an RFID tag $\mathcal{T}_j \in \mathcal{L}_i$ to retrieve $ID_{\mathcal{T}_j}$, $h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m$ and $h(\mathsf{ID}_{\mathcal{R}_i}, t_i)$, where $h^2(\mathsf{ID}_{\mathsf{CD}}, t_i)_m$ can also be retrieved without compromising the RFID tag.

- Step 2: $\mathcal{A}$ eavesdrops one session of the authentication phase of protocol between $\mathcal{R}_i$ (connected to $\mathcal{T}_j$) and CD but blocks the last messages from $\mathcal{R}_i$ to $\mathcal{T}_j$. It also stores $h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m$, $h(\mathsf{TS}\|\mathsf{ID}_K\|N_{\mathsf{CD}})$, N_{CD}, ID_K and $h(\mathsf{ID}_{\mathcal{T}_j}\|N_{\mathsf{CD}}\|\mathsf{ID}_{\mathcal{R}_i})$ that are transferred from CD to $\mathcal{R}_i$ over an insecure wireless channel that is easily accessible by the adversary.

CD **Impersonation Phase:** In this phase of the attack, to impersonate the target CD the adversary ($\mathcal{A}$) performs the following steps:

- Step 1: When R_i (connected to $\mathcal{T}_j$) sends the tuple: $(N'_{\mathcal{R}_i}, N'_{\mathcal{T}_j}, h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m, h\Big(h(\mathsf{ID}_{\mathcal{R}_i}, t_j)\|N'_{\mathcal{R}_i}\|N'_{\mathcal{T}_j}\Big) \oplus \mathsf{ID}_{\mathcal{T}_j}, \mathsf{ID}_{\mathcal{R}_i}, h(\mathsf{TS}\|N_{\mathcal{T}_j}\|N_{\mathcal{R}_i}))$ to the central database (CD) the adversary ($\mathcal{A}$) selects/calculates the following values:

$$\begin{aligned}
a' &:= h^2(\mathsf{ID}_{\mathsf{CD}}, t_i)_m\\
b' &:= h\Big(h(\mathsf{ID}_{\mathcal{R}_i}, t_i)\|N'_{\mathcal{R}_i}\|N'_{\mathcal{T}_j}\Big) \oplus \mathsf{ID}_{\mathcal{T}_i}\\
c &:= h(\mathsf{ID}_{\mathcal{T}_j}\|N_{\mathsf{CD}}\|\mathsf{ID}_{\mathcal{R}_i})\\
d &:= h(\mathsf{TS}\|\mathsf{ID}_K\|N_{\mathsf{CD}})\\
e &:= h(\mathsf{ID}_{\mathcal{T}_i}\|N'_{\mathcal{R}_i}\|N'_{\mathcal{T}_j}) \oplus \mathsf{ID}_K
\end{aligned}$$

and sends the tuple $(a', b', N_{\mathsf{CD}}, c, d, e)$ back to the RFID reader ($\mathcal{R}_i$).

- Step 2: The RFID reader ($\mathcal{R}_i$) verifies the correctness of the received value $c := h(\mathsf{ID}_{\mathcal{T}_j}\|N_{\mathsf{CD}}\|\mathsf{ID}_{\mathcal{R}_i})$, which is correct. Then, $\mathcal{R}_i$ finds the record of $\mathsf{ID}_{\mathcal{T}_j}$ as $\mathcal{T}_{CD}$ in its memory and extracts $\mathsf{ID}_{\mathcal{T}_i}$ as $\mathsf{ID}_{\mathcal{T}_{CD}}$, calculates ID_K from the value of $e := h(\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}}\|N'_{\mathcal{R}_i}\|N'_{\mathcal{T}_j}) \oplus \mathsf{ID}_K$ and verifies the correctness of the received value $d := h(\mathsf{TS}\|\mathsf{ID}_K\|N_{\mathsf{CD}})$ to authenticate the CD, which is also correct.

Hence, following the given attack, an active adversary ($\mathcal{A}$) who has compromised an RFID tag $\mathcal{T}_j \in \mathcal{L}_i$ can impersonate the CD efficiently. The success probability of the given attack is 1 while the attack complexity is compromising an RFID tag $\mathcal{T}_j$ and just two runs of the protocol.

B. READER IMPERSONATION ATTACK

As it mentioned already, in SMAP, RFID tags keep lower-level information while the central database (CD) keeps both lower-level information and the most valuable information of the system. Hence, if an adversary ($\mathcal{A}$) compromises an RFID tag, it can only receive lower-level information related to the RFID tag holder. However, if it can impersonate an RFID reader ($\mathcal{R}_i$) to the central database (CD) server (an RFID reader which has access to that RFID tag) then the adversary ($\mathcal{A}$) can retrieve all the information related to the RFID tag holder from the CD. Hence, it is very crucial for the protocol to withstand both RFID reader $\mathcal{R}_i$ and central database (CD) server impersonation attacks.

Nevertheless, we show that an adversary ($\mathcal{A}$) may impersonate an RFID reader ($\mathcal{R}_i$) to the central database (CD) server. To impersonate the RFID reader ($\mathcal{R}_i$), the adversary ($\mathcal{A}$) does as follows:

Learning Phase:

- Step 1: Assume that the adversary ($\mathcal{A}$) has already compromised M tags $(\mathcal{T}_1, \ldots, \mathcal{T}_M) \in \mathcal{L}_i$ to retrieve $\{(ID_{\mathcal{T}_j}, \mathsf{ID}_{\mathsf{CD}}, t_j)\}$, for $1 \le j \le M$, and aims to retrieve the higher-level information related to a compromised RFID tag. The adversary also generates the following list, based on the compromised tags' information:

$$\mathcal{L}'_i = \Big\{\Big(h(\mathsf{ID}_{\mathsf{CD}}, t_1)_m, h(\mathsf{ID}_{\mathcal{R}_i}, t_1), \mathsf{ID}_{\mathcal{T}_1}\Big), \ldots, \Big(h(\mathsf{ID}_{\mathsf{CD}}, t_M)_m, h(\mathsf{ID}_{\mathcal{R}_M}, t_M), \mathsf{ID}_{\mathcal{T}_M}\Big)\Big\}$$

- Step 2: $\mathcal{A}$ eavesdrops one session of the authentication phase of protocol between $\mathcal{R}_i$ (connected to any $\mathcal{T}_j$) and CD and stores $(ID_{\mathcal{R}_i}N_{\mathcal{R}_i}, N_{\mathcal{T}_j}, h(\mathsf{TS}\|N_{\mathcal{T}_j}\|N_{\mathcal{R}_i}))$ that are transferred from $\mathcal{R}_i$ to CD over an insecure wireless channel and easily accessible by the adversary.

RFID reader $\mathcal{R}_i$ Impersonation Phase:

In this phase of the attack, to impersonate the RFID reader ($\mathcal{R}_i$) and retrieve higher-level information of $\mathcal{T}_j$, for $1 \le j \le M$, the adversary ($\mathcal{A}$) does as follows:

- Step 1: $\mathcal{A}$ sends the tuple $(N_{\mathcal{R}_i}, N_{\mathcal{T}_j}, h^2(\mathsf{ID}_{\mathsf{CD}}, t_i)_m, h\Big(h(\mathsf{ID}_{\mathcal{R}_i}, t_i)\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j}\Big) \oplus \mathsf{ID}_{\mathcal{T}_j}, \mathsf{ID}_{\mathcal{R}_i}, h(\mathsf{TS}\|N_{\mathcal{T}_j}\|N_{\mathcal{R}_i}))$ to CD.

- Step 2: The central database (CD) receives the tuple sent by the adversary ($\mathcal{A}$) and verifies the correctness of the received value V. The value V is verified and CD finds $\mathcal{T}_j \in \mathcal{L}_i$ and chooses a random tag $\mathcal{T}_{\mathsf{CD}}$ from the access list $\mathcal{L}_i$ (of the reader $\mathcal{R}_i$) with identifier $\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}}$ and secret t_{CD}. The CD server also chooses a random identifier ID_K and a random nonce N_{CD}. Then, the central database (CD) server calculates the messages:

$$\begin{aligned}
a' &:= h^2(\mathsf{ID}_{\mathsf{CD}}, t_{\mathsf{CD}})_m\\
b' &:= h\Big(h(\mathsf{ID}_{\mathcal{R}_i}, t_{\mathsf{CD}})\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j}\Big) \oplus \mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}}\\
c &:= h(\mathsf{ID}_{\mathcal{T}_i}\|N_{\mathsf{CD}}\|\mathsf{ID}_{\mathcal{R}_i})\\
d &:= h(\mathsf{TS}\|\mathsf{ID}_K\|N_{\mathsf{CD}})\\
e &:= h(\mathsf{ID}_{\mathcal{T}_{\mathsf{CD}}}\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j}) \oplus \mathsf{ID}_K
\end{aligned}$$

and sends the tuple $(a', b', N_{\mathsf{CD}}, c, d, e)$ back to the RFID reader ($\mathcal{R}_i$) which is the adversary.

- Step 3: $\mathcal{A}$ selects a tag $\mathcal{T}'_{CD} \in \mathcal{L}'_i$ based on the received $h^2(\mathsf{ID}_{\mathsf{CD}}, t_{\mathsf{CD}})_m$, if there is any match, and calculates ID'_K as $\mathsf{ID}'_K := e \oplus h(\mathsf{ID}_{\mathcal{T}'_{\mathsf{CD}}}\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j})$. The adversary ($\mathcal{A}$) then selects a random $N_{\mathcal{T}_{j,2}}$ and sends the following tuple to the central database (CD) server:

$$\Big\{N_{\mathcal{T}_{j,2}}, h^2(\mathsf{ID}'_K, t_i)_m, h\Big(f(\mathsf{ID}_{\mathsf{CD}}, t_i)\|N_{\mathsf{CD}}\|N_{\mathcal{T}_{j,2}}\Big) \oplus \mathsf{ID}_{\mathcal{T}_j}\Big\}$$

- Step 5: The central database (CD) server receives the above mentioned tuple and verifies the correctness of the values $h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m$ and $h\Big(f(\mathsf{ID}_K, t_j)\|N_{\mathsf{CD}}\|N_{\mathcal{T}_{j,2}}\Big)$ (the former condition is confirmed with probability equal to 1). If these values are correct then $\mathcal{A}$ is authenticated as the RFID reader $\mathcal{R}_i$ to access the RFID tag ($\mathcal{T}_j$) and further information is transferred.

In the above attack, the adversary ($\mathcal{A}$) succeeds in the attack if the central database (CD) server selects $\mathcal{T}_{CD} \in \mathcal{L}'_i$ and the adversary ($\mathcal{A}$) makes a correct decision among the RFID tags in $\mathcal{L}'_i$ with the similar record of $h^2(\mathsf{ID}_{\mathsf{CD}}, t_{\mathsf{CD}})_m$. Assuming that the adversary ($\mathcal{A}$) has compromised M tags then, on average, each $\frac{M}{2^m}$ tags have a same record of $h^2(\mathsf{ID}_{\mathsf{CD}}, t_{\mathsf{CD}})_m$. In addition, the central database (CD) server selects an RFID tag $\mathcal{T}_{CD} \in \mathcal{L}'_i$ with the probability of $\frac{M}{n}$, where n is number of RFID tags in $\mathcal{L}_i$. Hence the success probability ($\mathbb{P}^{\mathsf{Imp}\mathcal{R}}_{M,1}$) of the given adversary ($\mathcal{A}$) to impersonate the RFID reader ($\mathcal{R}_i$) on each run of the above attack is determined as follows:

$$\mathbb{P}^{\mathsf{Imp}\mathcal{R}}_{M,1} = \frac{M}{n} \times \frac{1}{\max(1, \frac{M}{2^m})}$$

where, after q rounds of the described attack, the success probability ($\mathbb{P}^{\mathsf{Imp}\mathcal{R}}_{M,q}$) of the given adversary ($\mathcal{A}$) to impersonate the RFID reader ($\mathcal{R}_i$) is determined as follows:

$$\mathbb{P}^{\mathsf{Imp}\mathcal{R}}_{M,q} = 1-(1-\mathbb{P}^{\mathsf{Imp}\mathcal{R}}_{M,1})^q = 1-\left(1-\frac{M}{n} \times \frac{1}{\max(1, \frac{M}{2^m})}\right)^q$$

The success probability for $q \times M \approx n$ is expected to be non-negligible. For example, if $\frac{M}{2^m} \leq 1$ and $q \times M \approx n$ then $\mathbb{P}^{\mathsf{Imp}\mathcal{R}}_{M,q} = 1 - e^{-1}$.

IV. THE NEW STRONG ADVERSARY MODEL

In this section, we introduce a novel comprehensive adversary model which may be employed for the security analysis of any protocol for which the communication channel between the RFID reader $\mathcal{R}_i$ and the central database (CD) server is assumed to be insecure. In addition, we analyze the security of SMAP in this model.

A. RELATED ADVERSARY MODELS

Adversary who plays a main role in cryptanalysis of RFID security protocols can briefly categorized to three groups [29]: Passive adversary who can eavesdrop, intercept and replay protocols messages which are transferred over insecure channels. For example, in eavesdropping, it is not necessary to power RFID tag itself, so it can occur from large distance in comparison impersonating attacks [30]. Active adversary who can impersonate one of the protocols parties (i.e., tag, reader or back-end database) by using suitable devices (i.e. a rough reader for reader impersonation in the close proximity of a legitimate tag) and then communicate with the other protocol's party and in this line she can modify the transferred protocols messages. Putting impersonating devices in the close proximity of readers or tags is the main complexity of such attacks [30]. Moreover, modifying or blocking transferred messages can accomplished by using man in the middle devices [31].

Strong active adversary who has this ability to retrieve the tag and find out its identifier by producers same as physical reverse engineering and side channel attacks [29].

In this paper, the active adversary model is used in the first scenario of attack for central database impersonation attack and strong adversary model is used for reader impersonation attack and also second scenario of attack for central database impersonation attack.

In [32], the eight most well-known RFID privacy models are examined and compared. In these models, it is considered that the adversary is able to interact/play with an RFID tag in its neighborhood. These mentioned iterations are modeled by oracles. Among the generic oracles, $CORRUPT(T)$ returns the secret values of an RFID tag. All these models focus on the reader-tag channel, but the server-reader (or server-adversary) channel is not considered. As mentioned in Section I, there are many scenarios where we cannot assume a secure channel between the reader and the server. Moreover, a portion of the whole tag population can be compromised. This fact is what is studied in the proposed adversary model and it may easily be combined with the existing privacy models.

B. ADVERSARY MODEL

In this adversary model, we assume that the adversary ($\mathcal{A}$) has compromised some RFID tags for which the RFID reader ($\mathcal{R}_i$) has a record. Then, it should not increase the adversary's advantage for impersonating the RFID reader ($\mathcal{R}_i$) to the central database (CD) server or vice versa. We formally define the adversary's ($\mathcal{A}$) advantage to impersonate the RFID reader ($\mathcal{R}_i$) to the central database (CD) sever or vice versa as follows:

Definition 1: An authentication protocol for which the communication channel between the RFID reader ($\mathcal{R}_i$) and the central database (CD) server is insecure, it is said to be $(t_{\mathcal{A}}, M/n, q, \epsilon)$ compromised-tag-reader secure if for any polynomial-time (PPT) adversary $\mathcal{A}$, which has compromised at most M RFID tags of the whole population with n RFID tags $\mathcal{A}^{(\mathcal{T}_1 \ldots \mathcal{T}_M)}$, for its advantage to impersonate the RFID reader ($\mathcal{R}_i$) to the CD server (it outputs 1 if it does the attack successfully) it holds that:

$$\mathsf{Adv}^{\mathsf{Imp}}_{\mathcal{R}\to\mathcal{S}}(\mathcal{A}^{(\mathcal{T}_1 \ldots \mathcal{T}_M)}) = \left|\mathbb{P}\left[\mathcal{A}^{(\mathcal{T}_1 \ldots \mathcal{T}_M)} \Rightarrow 1\right] - \mathbb{P}\left[\mathcal{A} \Rightarrow 1\right]\right| \leq \epsilon$$

where $\mathcal{A}^{(\mathcal{T}_1 \ldots \mathcal{T}_M)}$ / $\mathcal{A}$ consumes at most polynomial time $t_{\mathcal{A}}$ and has access to at most q sessions of the protocol. The protocol is said to be (computationally) compromised-tag-reader security if the bound ϵ is a negligible function of the security parameter k, where k represents the total length of the secret parameters in the protocol. It must be noted that in this definition, $\mathcal{A}$ denotes an adversary which has not compromised any tag.

Definition 2: An authentication protocol for which the communication channel between the RFID reader ($\mathcal{R}_i$) and the central database (CD) server is insecure, is said to be $(t_{\mathcal{A}}, M/n, q, \epsilon)$ compromised-tag-server secure if for any PPT adversary $\mathcal{A}$, which has compromised at most M RFID tags out of the whole population of n RFID tags $\mathcal{A}^{(\mathcal{T}_1 \ldots \mathcal{T}_M)}$, for its advantage to impersonate the CD server to the RFID reader ($\mathcal{R}_i$) it holds that:

$$\begin{aligned}\mathsf{Adv}^{\mathsf{Imp}}_{\mathcal{S}\rightarrow\mathcal{R}}&(\mathcal{A}^{(\mathcal{T}_1 \ldots \mathcal{T}_M)})\\ &= \left|\mathbb{P}\left[\mathcal{A}^{(\mathcal{T}_1 \ldots \mathcal{T}_M)} \Rightarrow 1\right] - \mathbb{P}\left[\mathcal{A} \Rightarrow 1\right]\right| \leq \epsilon\end{aligned}$$

where $\mathcal{A}^{(\mathcal{T}_1 \ldots \mathcal{T}_M)}$ / $\mathcal{A}$ consumes at most polynomial time $t_{\mathcal{A}}$ and has access to at most q sessions of the protocol. The protocol is said to be (computationally) compromised-tag-server secure if the bound ϵ is a negligible function of the security parameter k, where k represents the total length of the secret parameters in the protocol.

Following the impersonation attack described in Section III-A, the adversary ($\mathcal{A}$)'s advantage to impersonate the CD server to the RFID reader ($\mathcal{R}_i$), when it has compromised an RFID tag, is "1". Hence, SMAP is $(t_{\mathcal{A}}, 1/n, 1, 1)$ compromised-tag-server secure where, $t_{\mathcal{A}}$ is a constant time to send the requested messages. In this attack, the hash function used in SMAP can be any hash function and we consider it as a random oracle.

To evaluate the SMAP security under the given adversary model and the random oracle model for the used hash function, against RFID reader impersonation attack we recall the attack which is presented in Section III-B. Following that attack, the adversary ($\mathcal{A}$)'s advantage to impersonate $\mathcal{R}_i$ after q runs of the protocol, when it has compromised M RFID tags, is lower bounded by $\mathbb{P}^{\mathsf{Imp}\mathcal{R}}_{M,q} = 1 - (1 - \mathbb{P}^{\mathsf{Imp}\mathcal{R}}_{M,1})^q = 1 - \left(1 - \frac{M}{n} \times \frac{1}{\max(1, \frac{M}{2m})}\right)^q$. Hence, SMAP is $(t_{\mathcal{A}}, M/n, q, \mathbb{P}^{\mathsf{Imp}\mathcal{R}}_{M,q})$ compromised-tag-server secure where, $t_{\mathcal{A}}$ is a constant time to calculate and send the requested messages.

The above analysis shows that SMAP is not a secure protocol under the given adversary model at all. The given adversary model is important because the valuable information is stored in the reader and the central database. Hence, by impersonating the reader, an adversary can reveal information from CD related to the compromised RFID tag which is not stored on the RFID tag's memory. On the other hand, by impersonating the CD server, the adversary ($\mathcal{A}$) can deceive the RFID reader ($\mathcal{R}_i$), e.g., forcing the RFID reader ($\mathcal{R}_i$) to send the tagged object to a wrong owner.

V. IMPROVEMENT OF SMAP

The first obvious weakness of SMAP is the way the central database (CD) uses to calculate its answer to the reader, i.e., $(a', b', N_{\mathsf{CD}}, c, d, e)$. In particular, it uses the information related to another tag when the target tag is being authenticated. This is a pitfall that unnecessarily discloses information related to a tag, which is not involved in the current session of the protocol. The second weakness resides in the fact that the adversary can use the messages sent by the reader and also the messages transferred in old sessions to satisfy parts of the expected answers from CD to $\mathcal{R}_i$. To overcome the above mentioned weaknesses, we embed a counter on each reader, denoted by $C_{\mathcal{R}_i}$ and initiated it by zero, and also keep a copy of it in CD (see Fig. 2). Moreover, we revise the exchanged messages between the involved entities in the server-mounted authentication phase of SMAP. Specifically, the revised scheme can be divided into the following steps:

- **Step 1:** The RFID reader ($\mathcal{R}_i$) has identified the RFID tag ($\mathcal{T}_j$) with identity $\mathsf{ID}_{\mathcal{T}_j}$. Then the RFID reader ($\mathcal{R}_i$) sends the tuple $(N_{\mathcal{R}_i}, N_{\mathcal{T}_j}, a, b, \mathsf{ID}_{\mathcal{R}_i}, V, C_{\mathcal{R}_i})$ to the central database (CD) and updates $C_{\mathcal{R}_i}$ by $C_{\mathcal{R}_i} + 1$, where:

$$\begin{aligned} a &:= h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m \\ b &:= h\Big(h(\mathsf{ID}_{\mathcal{R}_i}, t_j) \| N_{\mathcal{R}_i} \| N_{\mathcal{T}_j}\Big) \oplus \mathsf{ID}_{\mathcal{T}_j} \\ V &:= h(\mathsf{TS} \| N_{\mathcal{T}_j} \| N_{\mathcal{R}_i} \| C_{\mathcal{R}_i}) \end{aligned}$$

- **Step 2:** The central database (CD) receives the tuple sent by the RFID reader ($\mathcal{R}_i$) and verifies the correctness of the received value V and checks whether $(C_{\mathcal{R}_i})_{new} > (C_{\mathcal{R}_i})_{old}$, where $(C_{\mathcal{R}_i})_{new}$ is the sent value by the reader and $(C_{\mathcal{R}_i})_{old}$ is the record of $C_{\mathcal{R}_i}$ in CD. In case the received value V is not verified or $(C_{\mathcal{R}_i})_{old} \geq (C_{\mathcal{R}_i})_{new}$, the whole protocol aborts; otherwise, the central database (CD) using the access list $\mathcal{L}_i$ and the value a finds the tag's ($\mathcal{T}_j$) record and the related $\mathsf{ID}_{\mathcal{T}_j}$. Then, the central database (CD) generates a nonce N_{CD} and calculates the following messages:

$$\begin{aligned} c &:= h(\mathsf{TS} \| \mathsf{ID}_{\mathcal{T}_j} \| N_{\mathcal{R}_i} \| C_{\mathcal{R}_i}) \oplus N_{\mathsf{CD}} \\ d &:= h(\mathsf{ID}_{\mathcal{T}_j} \| \mathsf{TS} \| N_{\mathcal{T}_j} \| N_{\mathsf{CD}} \| N_{\mathcal{R}_i} \| C_{\mathcal{R}_i}) \end{aligned}$$

  Then, CD updates $C_{\mathcal{R}_i}$ by $(C_{\mathcal{R}_i})_{new}$ and sends the tuple (c, d) back to the RFID reader ($\mathcal{R}_i$).
- **Step 3:** The RFID reader ($\mathcal{R}_i$) extracts N_{CD} from the received value $c := h(\mathsf{TS} \| \mathsf{ID}_{\mathcal{T}_j} \| N_{\mathcal{R}_i} \| C_{\mathcal{R}_i}) \oplus N_{\mathsf{CD}}$ and verifies the correctness of the received value $d := h(\mathsf{TS} \| \mathsf{ID}_{\mathcal{T}_j} \| N_{\mathcal{T}_j} \| N_{\mathsf{CD}} \| N_{\mathcal{R}_i} \| C_{\mathcal{R}_i})$ to authenticate CD. Then the RFID reader ($\mathcal{R}_i$) sends N_{CD} and $\mathsf{ID}_{\mathcal{R}_i}$ to the RFID tag $\mathcal{T}_j$.
- **Step 4:** The RFID tag ($\mathcal{T}_j$) generates a new random nonce $N_{\mathcal{T}_{j,2}}$ and sends to the central database (CD) the tuple:

$$\Big\{N_{\mathcal{T}_{j,2}}, a' := h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m, \\ b' := h\Big(f(\mathsf{ID}_K, t_j) \| N_{\mathsf{CD}} \| N_{\mathcal{T}_{j,2}}\Big) \oplus \mathsf{ID}_{\mathcal{T}_j}\Big\}$$

- **Step 5:** The central database (CD) receives the above mentioned tuple and verifies the correctness of the values $a' := h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m$ and $b' := h\Big(f(\mathsf{ID}_{\mathcal{R}_i}, t_j) \| N_{\mathsf{CD}} \| N_{\mathcal{T}_{j,2}}\Big)$. If these values are correct

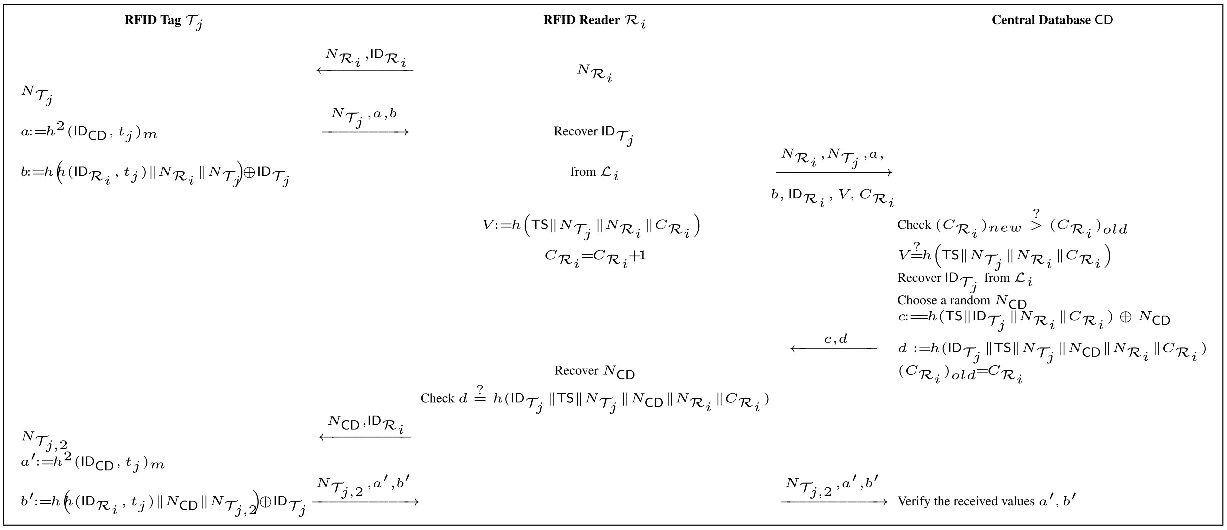

RFID Tag $\mathcal{T}_j$
RFID Reader $\mathcal{R}_i$
Central Database CD
$N_{\mathcal{R}_i}, \mathsf{ID}_{\mathcal{R}_i}$
$N_{\mathcal{R}_i}$
$N_{\mathcal{T}_j}$
$a{:=}h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m$
$b{:=}h\big(h(\mathsf{ID}_{\mathcal{R}_i}, t_j)\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j}\big)\oplus\mathsf{ID}_{\mathcal{T}_j}$
$N_{\mathcal{T}_j}, a, b$
Recover $\mathsf{ID}_{\mathcal{T}_j}$
from $\mathcal{L}_i$
$N_{\mathcal{R}_i}, N_{\mathcal{T}_j}, a,$
$b, \mathsf{ID}_{\mathcal{R}_i}, V, C_{\mathcal{R}_i}$
$V{:=}h\big(\mathsf{TS}\|N_{\mathcal{T}_j}\|N_{\mathcal{R}_i}\|C_{\mathcal{R}_i}\big)$
$C_{\mathcal{R}_i}{=}C_{\mathcal{R}_i}{+}1$
Check $(C_{\mathcal{R}_i})_{new} \overset{?}{>} (C_{\mathcal{R}_i})_{old}$
$V \overset{?}{=} h\big(\mathsf{TS}\|N_{\mathcal{T}_j}\|N_{\mathcal{R}_i}\|C_{\mathcal{R}_i}\big)$
Recover $\mathsf{ID}_{\mathcal{T}_j}$ from $\mathcal{L}_i$
Choose a random N_{CD}
$c{:=}h(\mathsf{TS}\|\mathsf{ID}_{\mathcal{T}_j}\|N_{\mathcal{R}_i}\|C_{\mathcal{R}_i}) \oplus N_{\mathsf{CD}}$
c, d
$d := h(\mathsf{ID}_{\mathcal{T}_j}\|\mathsf{TS}\|N_{\mathcal{T}_j}\|N_{\mathsf{CD}}\|N_{\mathcal{R}_i}\|C_{\mathcal{R}_i})$
$(C_{\mathcal{R}_i})_{old}{=}C_{\mathcal{R}_i}$
Recover N_{CD}
Check $d \overset{?}{=} h(\mathsf{ID}_{\mathcal{T}_j}\|\mathsf{TS}\|N_{\mathcal{T}_j}\|N_{\mathsf{CD}}\|N_{\mathcal{R}_i}\|C_{\mathcal{R}_i})$
$N_{\mathsf{CD}}, \mathsf{ID}_{\mathcal{R}_i}$
$N_{\mathcal{T}_{j,2}}$
$a'{:=}h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m$
$b'{:=}h\big(h(\mathsf{ID}_{\mathcal{R}_i}, t_j)\|N_{\mathsf{CD}}\|N_{\mathcal{T}_{j,2}}\big)\oplus\mathsf{ID}_{\mathcal{T}_j}$
$N_{\mathcal{T}_{j,2}}, a', b'$
$N_{\mathcal{T}_{j,2}}, a', b'$
Verify the received values a', b'

FIGURE 2. **ISMAP: the improved version of SMAP.**

then the RFID reader ($\mathcal{R}_i$) is authenticated to access the RFID tag $\mathcal{T}_j$ and further information is transferred.

A. ON THE SECURITY OF THE ISMAP

In the improved protocol, i.e. ISMAP, any exchanged message is randomized at least by one nonce, excluding $\Big(h(\mathsf{ID}_{\mathsf{CD}}, t_j)\Big)_m$ which remains identical as in the original SMAP and is shared between several tags. In addition, the authentication process of $\mathcal{T}_j$ does not reveal any information linked to $\mathcal{T}_i$, for any $\mathcal{T}_i \neq \mathcal{T}_j$. Moreover, the exchanged messages are selected such that any adversary has negligible advantage to reuse effectively a message transferred in the current session on a later session. The embedded counter $C_{\mathcal{R}_i}$ prevents the use of eavesdropped messages on later sessions. Hence the modified protocol provides a higher security level and overcomes the pitfalls of its predecessor. More precisely, our reasoning against common attacks is as follows:

1) TRACEABILITY

Although the structure of the message $a = h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m$ can be used to trace a group of tags, which is inherit from the original SMAP, the remaining messages are randomized by nonces and computed by an one way hash function such, which could be a lightweight hash function such as PHOTON [27] or Quark [28].Therefore it is not feasible for any adversary to link messages eavesdropped on the channel to a particular tag – or tag's holder. It should be noted such information has already been used to trace a tag, e.g. [26], [33]–[35] to trace the tag in a search protocol or [26] to trace the tag in the server-less version of Wang and Ma protocol. The main idea behind such a traceability is to send several queries and then determine whether the given tag is the target tag or not. However, it worth noting, in both SMAP and ISMAP, $a = h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m$ is used to reduce the server load and provide a scalable protocol. By reducing m, tracing a target tag gets harder but the reader/server task to identify the target tag uniquely will also increases. In this case, there is a trade off between the protocol efficiency and tag's privacy. For example, one can set $m = 0$, which means that the tag does not send $a = h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m$, then the adversary will not be able to trace the tag in this way. However, to identify the tag, the reader/server should do an exhaustive search over all tags in its list to find the target tag based on the received $b = h\Big(h(\mathsf{ID}_{\mathcal{R}_i}, t_j)\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j}\Big)\oplus\mathsf{ID}_{\mathcal{T}_j}$. It should be noted, in the revised protocol by Gao *et al.* [26], to reduce the reader/server cost they use a dynamic group index denoted by g_i and tag transfers $h(g_i)$. Although it is dynamic and can provide a better security against traceability attack, however, it could be used to distinguish tags from different groups, as far as they have not updated their group index.

In both SMAP and its improved version, ISMAP, the reader sends its identification value $\mathsf{ID}_{\mathcal{R}_i}$ over an insecure channel which can be used to trace the reader. Nevertheless, the privacy location of the reader was not one of the security requirements when the scheme was designed.

2) TAG IMPERSONATION

to impersonate a legitimate tag, an adversary should generate a valid pair $a = h^2(\mathsf{ID}_{\mathsf{CD}}, t_j)_m$ and $b = h\Big(h(\mathsf{ID}_{\mathcal{R}_i}, t_j)\|N_{\mathcal{R}_i}\|N_{\mathcal{T}_j}\Big) \oplus \mathsf{ID}_{\mathcal{T}_j}$. While it is possible for the adversary to create a valid a, however, it has a negligible chance to generate a valid b without the knowledge of $h(\mathsf{ID}_{\mathcal{R}_i}, t_j)$ and $\mathsf{ID}_{\mathcal{T}_j}$, given that $N_{\mathcal{R}_i}$ is contributed by the reader and is out of the adversary's control. Furthermore, if $\mathcal{T}_j$ is compromised, it does not help the adversary to impersonate $\mathcal{T}_i \neq \mathcal{T}_j$, because the private information of $\mathcal{T}_j$ does not reveal any information related to $\mathcal{T}_i$.

3) READER IMPERSONATION

to impersonate a legitimate reader to CD, an adversary should recover the contributed nonce by CD, i.e., N_{CD}, from $c = h(\mathsf{TS}\|\mathsf{ID}_{\mathcal{T}_j}\|N_{\mathcal{R}_i}\|C_{\mathcal{R}_i}) \oplus N_{\mathsf{CD}}$ and send it to $\mathcal{T}_j$.

TABLE 2. Security comparison of SMAP and ISMAP, where A_1, A_2, A_3, A_4, A_5 and A_6 respectively denote security against tag impersonation attack, reader impersonation attack, CD impersonation attack, traceability attack, desynchronization attack and the new adversary model.

Protocol	A_1	A_2	A_3	A_4	A_5	A_6
SMAP	✓	×	×	parietal	✓	×
ISMAP	✓	✓	✓	parietal	✓	✓

However, to recover that nonce, the adversary needs TS and $\mathsf{ID}_{\mathcal{T}_j}$ that are private values. In addition, the reader cannot just replay the eavesdropped messages from an old session in a later one, due to the increasing counter $C_{\mathcal{R}_i}$. On the other hand, compromising $\mathcal{T}_j$ or any number of tags, does not help the adversary to impersonate the reader and receive high level information related to the compromised tag or other tags from the CD. The reason is the fact that to complete the authentication process an adversary at least needs the knowledge of TS, which is not extractable from any compromised tag or exchanged messages over channel.

4) SERVER IMPERSONATION

to impersonate a legitimate server to $\mathcal{R}_i$, an adversary should generate a valid pair of $c = h(\mathsf{TS}\|\mathsf{ID}_{\mathcal{T}_j}\|N_{\mathcal{R}_i}\|C_{\mathcal{R}_i}) \oplus N_{\mathsf{CD}}$ and $d = h(\mathsf{ID}_{\mathcal{T}_j}\|\mathsf{TS}\|N_{\mathcal{T}_j}\|N_{\mathsf{CD}}\|N_{\mathcal{R}_i}\|C_{\mathcal{R}_i})$ where $N_{\mathcal{R}_i}$ is contributed by the reader and TS is a secret parameter only known by the legitimate reader and CD. Therefore any adversary has a negligible advantage to impersonate CD.

5) NEW ADVERSARY MODEL

In ISMAP, compromising $\mathcal{T}_j$ or any number of tags, does not help the adversary to impersonate the server to the reader. This is due to the fact that to impersonate the server, the adversary at least needs the knowledge of TS which is not extractable from any compromised tag or transferred messages over channel.

6) DE-SYNCHRONIZATION ATTACK

The only parameter which is updated and could lead to desynchronize the reader from CD is $C_{\mathcal{R}_i}$. However, to do so, the adversary either should impersonate the reader which is not feasible or block many queries from reader to CD such that the counter overflows and restarts from zero which is also impractical assuming that the length of the counter is enough large (e.g., 64 bits).

7) SECURITY COMPARISON

In Table 2, the security of ISMAP is compared with SMAP against different attacks, which shows that ISMAP provides better security against different attacks.

B. FORMAL SECURITY ANALYSIS OF ISMAP

So far, several formal methods have been developed to evaluate the robustness of a cryptographic protocol. Formal methods are either manual such as GNY logic [36], SVO [37], and BAN logic [38] or automatic such as AVISPA [39], Proverif [40], CryptoVerif [41] and Scyther [42]. In this section, we evaluate the security of ISMAP using GNY logic and the Scyther tool, which are widely accepted methods to formally evaluate the security of a cryptographic protocol and have been used to evaluate the security of many protocols so far, e.g. [43]–[48].

1) GNY LOGIC PROOF

To evaluate the security of a protocol using GNY logic, an analyzer should follow several steps, that are as follows:

- The messages of the protocol are expressed in the GNY logic form.
- The messages of the protocol will be idealized, where the messages that are plain or do not increase the confidentiality are deleted.
- Proper security assumptions and security goals of the protocol are expressed.
- Finally, based on the GNY logic rules, the security goals are deduced from idealized messages and also the protocol assumptions.

Here, based on the notations that are represented in Table 3, the robustness of ISMAP is deduced using GNY logic, as follows:

- The messages of ISMAP are written using GNY logic notations. Table 4 represents the ISMAP messages in GNY logic format.
- In this step, which is the idealization step of the proof, plain messages of ISMAP are deleted. Table 5 shows the output of this step for ISMAP.
- In this step, the ISMAP's assumptions and security goals are expressed. Table 6 shows the output of this step for ISMAP.
- Ultimately, using messages and protocol assumptions and based on the GNY logic rules, we deduce the desired security goals. Table 7 represents the output of this step for ISMAP protocol.

Based on Table 7, given, $A13$ and $F1$, we can deduce that $D1 : \mathsf{CD}| \equiv \sharp\{N_{\mathcal{T}_j}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}$. Using $A15$, based on $R1$, we retrieve that $D2 : \mathsf{CD}| \equiv \phi(\{N_{\mathcal{T}_j}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\})$. Using $IM3$, $A32$, $A23$, $D2$, $D1$ and based on $I1$, we deduce that $D3 : \mathsf{CD}| \equiv \mathcal{R}_i| \sim \{N_{\mathcal{T}_j}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}$. Considering $D3$ and based on $I7$, we retrieve that $D4 : \mathsf{CD}| \equiv \mathcal{R}_i| \sim N_{\mathcal{R}_i}$. Since $I1$ has three outputs, using $IM3$, $A32$, $A23$, $D2$, $D1$ and based on $I1$, we also deduce that $D5 : \mathsf{CD}| \equiv \mathcal{R}_i \ni \{N_{\mathcal{T}_j}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}$. Considering $D5$ based on $P3$ results $D6 : \mathsf{CD}| \equiv \mathcal{R}_i \ni N_{\mathcal{T}_j}$.

Given, $A7$, based on $F1$, we deduce that $D7 : \mathcal{R}_i| \equiv \sharp\{\mathsf{ID}_{\mathcal{T}_j}, N_{\mathcal{T}_j}, N_{\mathsf{CD}}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}$. Using $A9$, based on $R1$, we retrieve that $D8 : \mathcal{R}_i| \equiv \phi(\{\mathsf{ID}_{\mathcal{T}_j}, N_{\mathcal{T}_j}, N_{\mathsf{CD}}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\})$. Using $IM4$,$A31$, $A22$, $D8$, $D7$ and based on $I1$, we deduce that $D9 : \mathcal{R}_i| \equiv \mathsf{CD}| \sim \{\mathsf{ID}_{\mathcal{T}_j}, N_{\mathcal{T}_j}, N_{\mathsf{CD}}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}$. Considering $D9$ and based on $I7$, we retrieve that $D10 : \mathcal{R}_i| \equiv \mathsf{CD}| \sim N_{\mathsf{CD}}$. Since $I1$ has three outputs, using $IM4$, $A31$, $A22$, $D8$, $D7$ and based on $I1$, we also deduce that $D11 : \mathcal{R}_i| \equiv \mathsf{CD} \ni \{\mathsf{ID}_{\mathcal{T}_j}, N_{\mathcal{T}_j}, N_{\mathsf{CD}}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}$. Considering $D11$ based on $P3$ results $D12 : \mathcal{R}_i| \equiv$

TABLE 3. GNY logic notations and rules that are used in this paper.

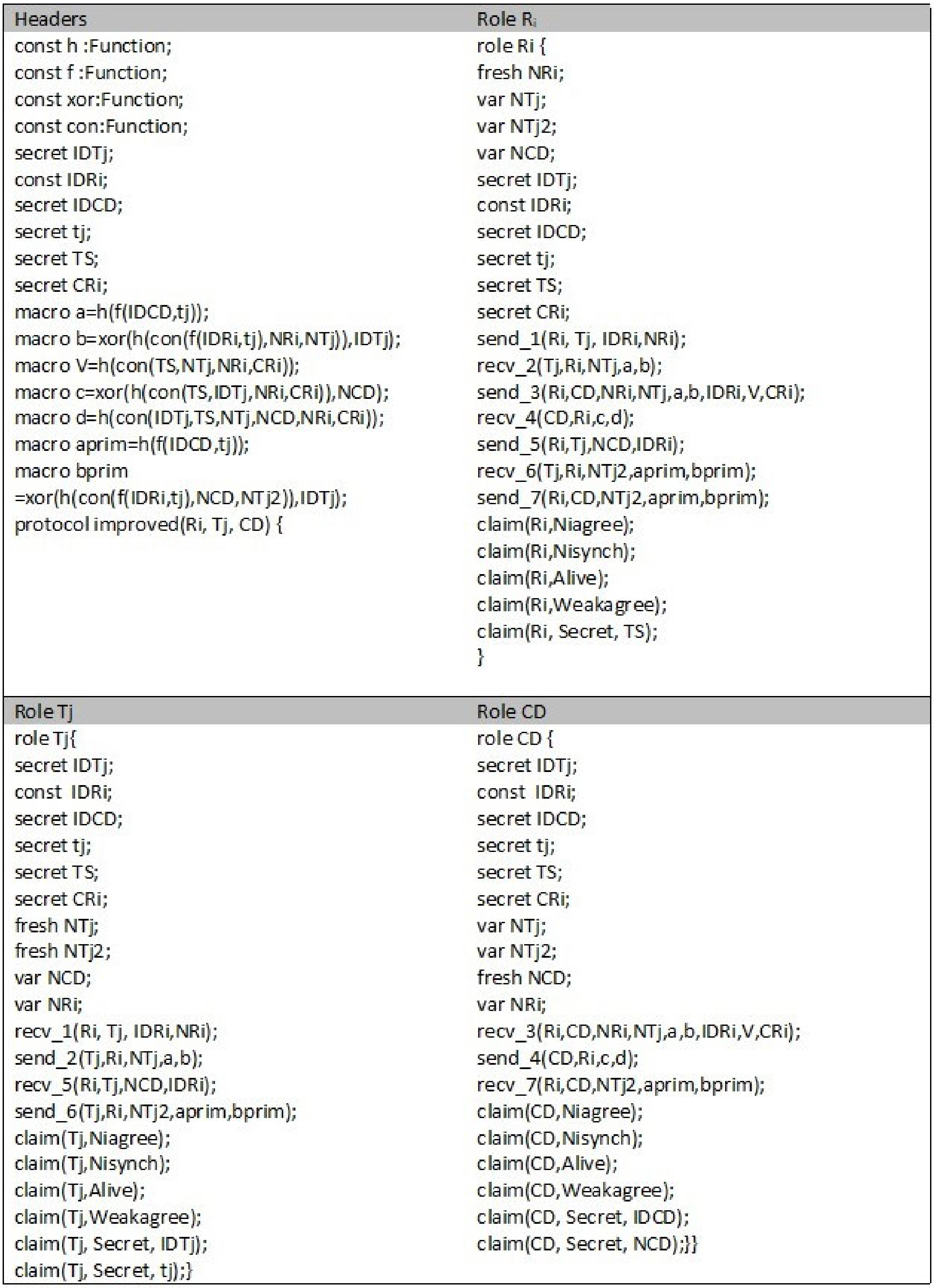
Notations	Description
$\sharp(X)$	The message X is fresh
$\{X\}_K$	The message X is encrypted using K as the key
$P \lhd X$	P receives the message X
$P \xleftrightarrow{K} Q$	K is securely shared between P and Q
$P \ni K$	P possesses K
$\phi(X)$	shows recognizability of X
$*(X)$	X was not originated by the party who receives it.
$F1 : \dfrac{P\vert\equiv \sharp(X)}{P\vert\equiv \sharp(X,Y), P\vert\equiv \sharp(F(X))}$	Means that if P believes freshness of X, then it deduced that P believes freshness of any formula of X.
$I7 : \dfrac{P\vert\equiv Q\vert\sim(X,Y)}{P\vert\equiv Q\vert\sim(X)}$	Means if P believes Q has sent a set of messages it deduced that P believes Q has sent each of messages also.
$P3 : \dfrac{P \ni (X,Y)}{P \ni (X)}$	Means that if P possesses a formula, it also possesses each of the formula components.
$R1 : \dfrac{P\vert\equiv \phi(X)}{P\vert\equiv \phi(X,Y), P\vert\equiv \phi(F(X))}$	Means that if P believes recognizability of X, then it deduced that P believes recognizability of any formula of X.
$I1 : \dfrac{A}{B}$, where $A : P \lhd *\{X\}_K, P \ni K, P\vert\equiv P \xleftrightarrow{K} Q$, $P\vert\equiv \phi(X), P\vert\equiv \sharp(X,K)$ and $B : P\vert\equiv Q\vert\sim X, P\vert\equiv Q\vert\sim\{X\}_K, P\vert\equiv Q \ni X$	Means that if P receives a message X which is encrypted with K and was not originated by itself, and he possesses K and he believes K is a shared secret between itself and Q, also believes recognizability of X and also believes freshness of X or K, then it is deduced that P believes Q sent X, and also believes Q sent the encrypted message of X with K and also believes Q possesses X.

TABLE 4. GNY logic expression of ISMAP messages.

No. of messages	Description
M_1	$\mathcal{T}_j \lhd *N_{\mathcal{R}_i}, *\mathsf{ID}_{\mathcal{R}_i}$
M_2	$R_i \lhd *N_{\mathcal{T}_j}, *a = \{\mathsf{ID}_{\mathsf{CD}}\}_{t_j}, *b = \{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathcal{R}_i}, N_{\mathcal{T}_j}, \mathsf{ID}_{\mathcal{T}_j}\}_{t_j}$
M_3	$\mathsf{CD} \lhd *N_{\mathcal{R}_i}, *N_{\mathcal{T}_j}, *a = \{\mathsf{ID}_{\mathsf{CD}}\}_{t_j}, *b = \{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathcal{R}_i}, N_{\mathcal{T}_j}, \mathsf{ID}_{\mathcal{T}_j}\}_{t_j}, \mathsf{ID}_{\mathcal{R}_i}, *V = \{N_{\mathcal{T}_j}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}_{TS}, C_{\mathcal{R}_i}$
M_4	$R_i \lhd *c = \{\mathsf{ID}_{\mathcal{T}_j}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}, N_{\mathsf{CD}}\}_{TS}$,$*d = \{\mathsf{ID}_{\mathcal{T}_j}, N_{\mathcal{T}_j}, N_{\mathsf{CD}}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}_{TS}$
M_5	$\mathcal{T}_j \lhd *N_{\mathsf{CD}}, *\mathsf{ID}_{\mathcal{R}_i}$
M_6	$R_i \lhd *N_{\mathcal{T}_{j,2}}, *a' = \{\mathsf{ID}_{\mathsf{CD}}\}_{t_j}, *b' = \{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathsf{CD}}, N_{\mathcal{T}_{j,2}}, \mathsf{ID}_{\mathcal{T}_j}\}_{t_j}$
M_7	$\mathsf{CD} \lhd *N_{\mathcal{T}_{j,2}}, *a' = \{\mathsf{ID}_{\mathsf{CD}}\}_{t_j}, *b' = \{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathsf{CD}}, N_{\mathcal{T}_{j,2}}, \mathsf{ID}_{\mathcal{T}_j}\}_{t_j}$

TABLE 5. ISMAP messages idealization.

No. of messages	Description
IM_2	$R_i \lhd *\{\mathsf{ID}_{\mathsf{CD}}\}_{t_j}, *\{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathcal{R}_i}, N_{\mathcal{T}_j}, \mathsf{ID}_{\mathcal{T}_j}\}_{t_j}$
IM_3	$\mathsf{CD} \lhd *\{\mathsf{ID}_{\mathsf{CD}}\}_{t_j}, *\{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathcal{R}_i}, N_{\mathcal{T}_j}, \mathsf{ID}_{\mathcal{T}_j}\}_{t_j}, *\{N_{\mathcal{T}_j}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}_{TS}$
IM_4	$R_i \lhd *\{\mathsf{ID}_{\mathcal{T}_j}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}, N_{\mathsf{CD}}\}_{TS}$,$*\{\mathsf{ID}_{\mathcal{T}_j}, N_{\mathcal{T}_j}, N_{\mathsf{CD}}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}_{TS}$
IM_6	$R_i \lhd *\{\mathsf{ID}_{\mathsf{CD}}\}_{t_j}, *\{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathsf{CD}}, N_{\mathcal{T}_{j,2}}, \mathsf{ID}_{\mathcal{T}_j}\}_{t_j}$
IM_7	$\mathsf{CD} \lhd *\{\mathsf{ID}_{\mathsf{CD}}\}_{t_j}, *\{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathsf{CD}}, N_{\mathcal{T}_{j,2}}, *\mathsf{ID}_{\mathcal{T}_j}\}_{t_j}$



Headers

```
const h :Function;
const f :Function;
const xor:Function;
const con:Function;
secret IDTj;
const IDRi;
secret IDCD;
secret tj;
secret TS;
secret CRi;
macro a=h(f(IDCD,tj));
macro b=xor(h(con(f(IDRi,tj),NRi,NTj)),IDTj);
macro V=h(con(TS,NTj,NRi,CRi));
macro c=xor(h(con(TS,IDTj,NRi,CRi)),NCD);
macro d=h(con(IDTj,TS,NTj,NCD,NRi,CRi));
macro aprim=h(f(IDCD,tj));
macro bprim
=xor(h(con(f(IDRi,tj),NCD,NTj2)),IDTj);
protocol improved(Ri, Tj, CD) {
```

Role Ri

```
role Ri {
fresh NRi;
var NTj;
var NTj2;
var NCD;
secret IDTj;
const IDRi;
secret IDCD;
secret tj;
secret TS;
secret CRi;
send_1(Ri, Tj, IDRi,NRi);
recv_2(Tj,Ri,NTj,a,b);
send_3(Ri,CD,NRi,NTj,a,b,IDRi,V,CRi);
recv_4(CD,Ri,c,d);
send_5(Ri,Tj,NCD,IDRi);
recv_6(Tj,Ri,NTj2,aprim,bprim);
send_7(Ri,CD,NTj2,aprim,bprim);
claim(Ri,Niagree);
claim(Ri,Nisynch);
claim(Ri,Alive);
claim(Ri,Weakagree);
claim(Ri, Secret, TS);
}
```

Role Tj

```
role Tj{
secret IDTj;
const  IDRi;
secret IDCD;
secret tj;
secret TS;
secret CRi;
fresh NTj;
fresh NTj2;
var NCD;
var NRi;
recv_1(Ri, Tj, IDRi,NRi);
send_2(Tj,Ri,NTj,a,b);
recv_5(Ri,Tj,NCD,IDRi);
send_6(Tj,Ri,NTj2,aprim,bprim);
claim(Tj,Niagree);
claim(Tj,Nisynch);
claim(Tj,Alive);
claim(Tj,Weakagree);
claim(Tj, Secret, IDTj);
claim(Tj, Secret, tj);}
```

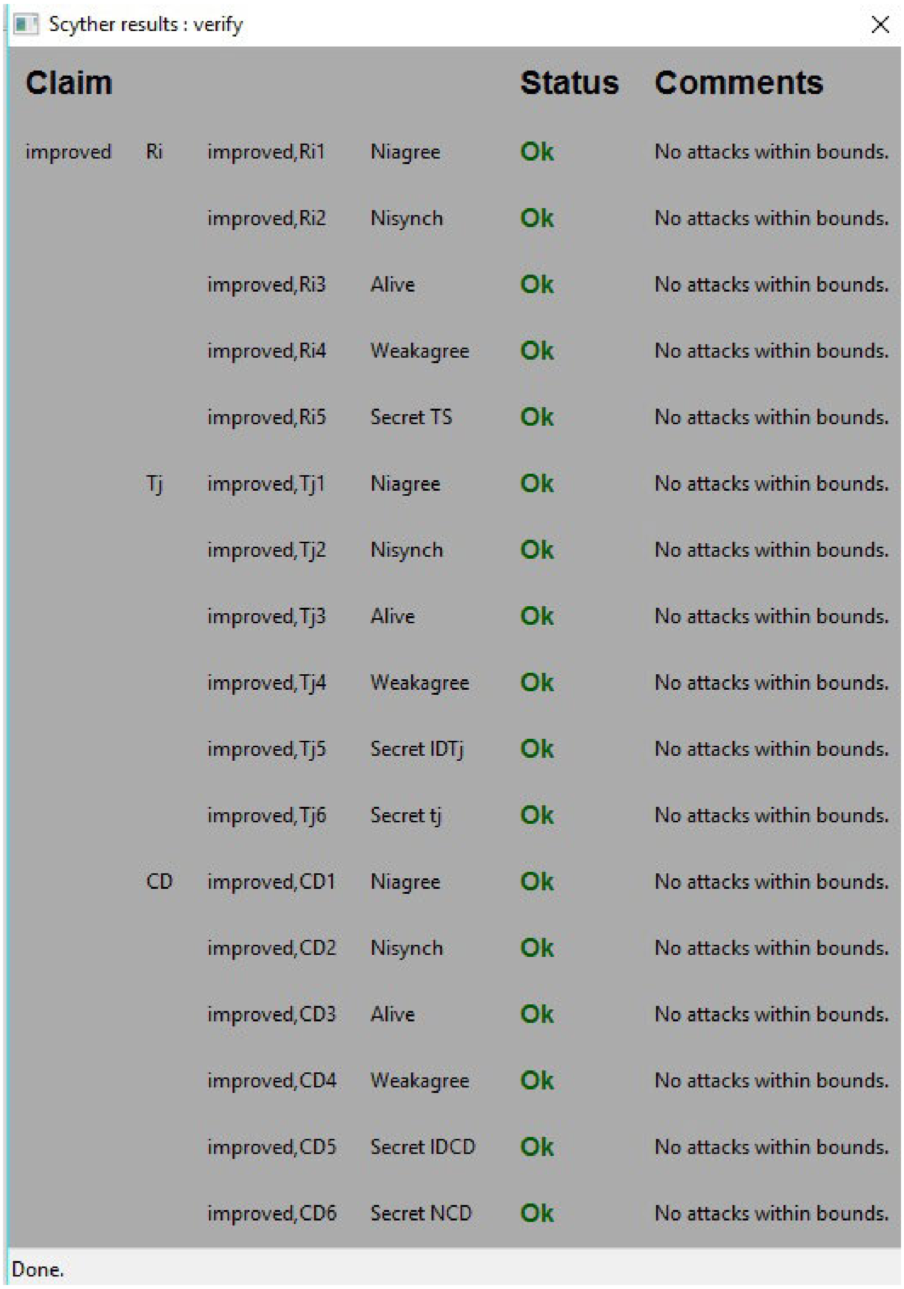
Role CD

```
role CD {
secret IDTj;
const  IDRi;
secret IDCD;
secret tj;
secret TS;
secret CRi;
var NTj;
var NTj2;
fresh NCD;
var NRi;
recv_3(Ri,CD,NRi,NTj,a,b,IDRi,V,CRi);
send_4(CD,Ri,c,d);
recv_7(Ri,CD,NTj2,aprim,bprim);
claim(CD,Niagree);
claim(CD,Nisynch);
claim(CD,Alive);
claim(CD,Weakagree);
claim(CD, Secret, IDCD);
claim(CD, Secret, NCD);}}
```

FIGURE 3. **Reprenstiation of ISMAP in the SPDL.**

$CD \ni N_{\mathcal{T}_j}$. Given $D11$ based on $P3$ also results $D13 : \mathcal{R}_i| \equiv \mathsf{CD} \ni N_{\mathcal{R}_i}$.

Given, $A10$, based on $F1$, we deduce that $D14 : \mathsf{CD}| \equiv \sharp\{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathsf{CD}}, N_{\mathcal{T}_{j,2}}, \mathsf{ID}_{\mathcal{T}_j}\}$. Using $A12$, based on $R1$, we retrieve that $D15 : \mathsf{CD}| \equiv \phi(\{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathsf{CD}}, N_{\mathcal{T}_{j,2}}, \mathsf{ID}_{\mathcal{T}_j}\})$. Using $IM7, A27, A17, D15, D14$ and based on $I1$, we deduce that $D16 : \mathsf{CD}| \equiv \mathcal{T}_j| \sim \{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathsf{CD}}, N_{\mathcal{T}_{j,2}}, \mathsf{ID}_{\mathcal{T}_j}\}$. Considering $D16$ and based on $I7$, we retrieve that $D17 : \mathsf{CD}| \equiv \mathcal{T}_j| \sim N_{\mathcal{T}_{j,2}}$. Since $I1$ has three outputs, using $IM7$,$A27$, $A17$, $D15$, $D14$ and based on $I1$, we also deduce that $D18 : \mathsf{CD}| \equiv \mathcal{T}_j \ni \{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathsf{CD}}, N_{\mathcal{T}_{j,2}}, \mathsf{ID}_{\mathcal{T}_j}\}$. Considering $D18$ based on $P3$ results $D19 : \mathsf{CD}| \equiv \mathcal{T}_j \ni N_{\mathsf{CD}}$.



Scyther results : verify

Claim				Status	Comments
improved	Ri	improved,Ri1	Niagree	Ok	No attacks within bounds.
		improved,Ri2	Nisynch	Ok	No attacks within bounds.
		improved,Ri3	Alive	Ok	No attacks within bounds.
		improved,Ri4	Weakagree	Ok	No attacks within bounds.
		improved,Ri5	Secret TS	Ok	No attacks within bounds.
	Tj	improved,Tj1	Niagree	Ok	No attacks within bounds.
		improved,Tj2	Nisynch	Ok	No attacks within bounds.
		improved,Tj3	Alive	Ok	No attacks within bounds.
		improved,Tj4	Weakagree	Ok	No attacks within bounds.
		improved,Tj5	Secret IDTj	Ok	No attacks within bounds.
		improved,Tj6	Secret tj	Ok	No attacks within bounds.
	CD	improved,CD1	Niagree	Ok	No attacks within bounds.
		improved,CD2	Nisynch	Ok	No attacks within bounds.
		improved,CD3	Alive	Ok	No attacks within bounds.
		improved,CD4	Weakagree	Ok	No attacks within bounds.
		improved,CD5	Secret IDCD	Ok	No attacks within bounds.
		improved,CD6	Secret NCD	Ok	No attacks within bounds.

Done.

FIGURE 4. The results of security verification of ISMAP in the Scyther tool.

$G1$ indicates that the random number, i.e. $N_{\mathcal{R}_i}$ which is sent by $\mathcal{R}_i$, is not changed through insecure channel and is received unchanged by CD.

$G2$ shows that CD believes $\mathcal{R}_i$ possesses $N_{\mathcal{T}_j}$ which means CD believes $\mathcal{R}_i$ can compute and verify any formula including $N_{\mathcal{T}_j}$.

$G3$ indicates that the random number N_{CD}, which is sent by CD, has not been changed through insecure channel and it is received unchanged by R_i and R_i believes that what it has received as N_{CD} is the same N_{CD} which has been sent by CD.

$G4$ shows that $\mathcal{R}_i$ believes CD possesses $N_{\mathcal{T}_j}$ which means $\mathcal{R}_i$ believes that CD can compute and verify any formula including $N_{\mathcal{T}_j}$.

$G5$ shows that $\mathcal{R}_i$ believes CD possesses $N_{\mathcal{R}_i}$ which means $\mathcal{R}_i$ believes that CD can compute and verify any formula including $N_{\mathcal{R}_i}$.

$G6$ indicates that the random number $N_{\mathcal{T}_{j,2}}$, which is sent by $\mathcal{T}_j$, is not changed through insecure channel and it is received unchanged by CD and CD believes that what it has received as $N_{\mathcal{T}_{j,2}}$ is the same $N_{\mathcal{T}_{j,2}}$ which has been sent by $\mathcal{T}_j$.

$G7$ shows that CD believes $\mathcal{T}_j$ possesses N_{CD} which means CD believes $\mathcal{T}_j$ can compute and verify any formula including N_{CD}.

Following the above argument, we can conclude that, based on the GNY logic, ISMAP provides desired security against various attacks.

TABLE 6. ISMAP assumption and security goals.

No. of Assumption/Goal	Description	No. of Assumption/Goal	Description
$A1$	$\mathcal{T}_j\vert \equiv \sharp N_{\mathcal{T}_j}$	$A2$	$\mathcal{T}_j \ni N_{\mathcal{T}_j}$
$A3$	$\mathcal{T}_j\vert \equiv \phi(N_{\mathcal{T}_j})$	$A4$	$\mathcal{T}_j\vert \equiv \sharp N_{\mathcal{T}_{j,2}}$
$A5$	$\mathcal{T}_j \ni N_{\mathcal{T}_{j,2}}$	$A6$	$\mathcal{T}_j\vert \equiv \phi(N_{\mathcal{T}_{j,2}})$
$A7$	$R_i\vert \equiv \sharp N_{\mathcal{R}_i}$	$A8$	$R_i \ni N_{\mathcal{R}_i}$
$A9$	$R_i\vert \equiv \phi(N_{\mathcal{R}_i})$	$A10$	$\mathsf{CD}\vert \equiv \sharp N_{\mathsf{CD}}$
$A11$	$\mathsf{CD} \ni N_{\mathsf{CD}}$	$A12$	$\mathsf{CD}\vert \equiv \phi(N_{\mathsf{CD}})$
$A13$	$\mathsf{CD}\vert \equiv \sharp C_{\mathcal{R}_i}$	$A14$	$\mathsf{CD} \ni C_{\mathcal{R}_i}$
$A15$	$\mathsf{CD}\vert \equiv \phi(C_{\mathcal{R}_i})$	$A16$	$\mathcal{T}_j\vert \equiv \mathcal{T}_j \overset{\mathsf{ID}_{\mathcal{T}_j},t_j}{\longleftrightarrow} \mathsf{CD}$
$A17$	$\mathsf{CD}\vert \equiv \mathsf{CD} \overset{\mathsf{ID}_{\mathcal{T}_j},t_j}{\longleftrightarrow} \mathcal{T}_j$	$A18$	$\mathcal{T}_j\vert \equiv \mathcal{T}_j \overset{\mathsf{ID}_{\mathcal{T}_j}}{\longleftrightarrow} R_i$
$A19$	$R_i\vert \equiv R_i \overset{\mathsf{ID}_{\mathcal{T}_j}}{\longleftrightarrow} \mathcal{T}_j$	$A20$	$\mathsf{CD}\vert \equiv \mathsf{CD} \overset{\mathsf{ID}_{\mathsf{CD}}}{\longleftrightarrow} \mathcal{T}_j$
$A21$	$\mathcal{T}_j\vert \equiv \mathcal{T}_j \overset{\mathsf{ID}_{\mathsf{CD}}}{\longleftrightarrow} \mathsf{CD}$	$A22$	$R_i\vert \equiv R_i \overset{TS}{\longleftrightarrow} \mathsf{CD}$
$A23$	$\mathsf{CD}\vert \equiv \mathsf{CD} \overset{TS}{\longleftrightarrow} R_i$	$A24$	$\mathcal{T}_j \ni \mathsf{ID}_{\mathcal{T}_j}$
$A25$	$\mathcal{T}_j \ni t_j$	$A26$	$\mathsf{CD} \ni \mathsf{ID}_{\mathcal{T}_j}$
$A27$	$\mathsf{CD} \ni t_j$	$A28$	$R_i \ni \mathsf{ID}_{\mathcal{T}_j}$
$A29$	$\mathsf{CD} \ni \mathsf{ID}_{\mathsf{CD}}$	$A30$	$\mathcal{T}_j \ni \mathsf{ID}_{\mathsf{CD}}$
$A31$	$\mathcal{R}_i \ni \mathsf{TS}$	$A32$	$\mathsf{CD} \ni \mathsf{TS}$
$G1$	$\mathsf{CD}\vert \equiv \mathcal{R}_i\vert \sim N_{\mathcal{R}_i}$	$G2$	$\mathsf{CD}\vert \equiv \mathcal{R}_i \ni N_{\mathcal{T}_j}$
$G3$	$\mathcal{R}_i\vert \equiv \mathsf{CD}\vert \sim N_{\mathsf{CD}}$	$G4$	$\mathcal{R}_i\vert \equiv \mathsf{CD} \ni N_{\mathcal{T}_j}$
$G5$	$\mathcal{R}_i\vert \equiv \mathsf{CD} \ni N_{\mathcal{R}_i}$	$G6$	$\mathsf{CD}\vert \equiv \mathcal{T}_j\vert \sim N_{\mathcal{T}_{j,2}}$
$G7$	$\mathsf{CD}\vert \equiv \mathcal{T}_j \ni N_{\mathsf{CD}}$	-	-

TABLE 7. ISMAP security goals deduction.

Deduction No.	Given messages and assumptions	Used rule	Deduction Description	Goal No.
$D1$	$A13$	$F1$	$\mathsf{CD}\vert \equiv \sharp\{N_{\mathcal{T}_j}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}$	–
$D2$	$A15$	$R1$	$\mathsf{CD}\vert \equiv \phi(\{N_{\mathcal{T}_j}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\})$	–
$D3$	$IM3$, $A32$,$A23$,$D2$,$D1$	$I1$	$\mathsf{CD}\vert \equiv \mathcal{R}_i\vert \sim \{N_{\mathcal{T}_j}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}$	–
$D4$	$D3$	$I7$	$\mathsf{CD}\vert \equiv \mathcal{R}_i\vert \sim N_{\mathcal{R}_i}$	$G1$
$D5$	$IM3$, $A32$,$A23$,$D2$,$D1$	$I1$	$\mathsf{CD}\vert \equiv \mathcal{R}_i \ni \{N_{\mathcal{T}_j}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}$	–
$D6$	$D5$	$P3$	$\mathsf{CD}\vert \equiv \mathcal{R}_i \ni N_{\mathcal{T}_j}$	$G2$
$D7$	$A7$	$F1$	$\mathcal{R}_i\vert \equiv \sharp\{\mathsf{ID}_{\mathcal{T}_j}, N_{\mathcal{T}_j}, N_{\mathsf{CD}}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}$	–
$D8$	$A9$	$R1$	$\mathcal{R}_i\vert \equiv \phi(\{\mathsf{ID}_{\mathcal{T}_j}, N_{\mathcal{T}_j}, N_{\mathsf{CD}}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}$	–
$D9$	$IM4$, $A31$,$A22$,$D8$,$D7$	$I1$	$\mathcal{R}_i\vert \equiv \mathsf{CD}\vert \sim \{\mathsf{ID}_{\mathcal{T}_j}, N_{\mathcal{T}_j}, N_{\mathsf{CD}}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}$	–
$D10$	$D9$	$I7$	$\mathcal{R}_i\vert \equiv \mathsf{CD}\vert \sim N_{\mathsf{CD}}$	$G3$
$D11$	$IM4$, $A31$,$A22$,$D8$,$D7$	$I1$	$\mathcal{R}_i\vert \equiv \mathsf{CD} \ni \{\mathsf{ID}_{\mathcal{T}_j}, N_{\mathcal{T}_j}, N_{\mathsf{CD}}, N_{\mathcal{R}_i}, C_{\mathcal{R}_i}\}$	–
$D12$	$D11$	$P3$	$\mathcal{R}_i\vert \equiv \mathsf{CD} \ni N_{\mathcal{T}_j}$	$G4$
$D13$	$D11$	$P3$	$\mathcal{R}_i\vert \equiv \mathsf{CD} \ni N_{\mathcal{R}_i}$	$G5$
$D14$	$A10$	$F1$	$\mathsf{CD}\vert \equiv \sharp\{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathsf{CD}}, N_{\mathcal{T}_{j,2}}, \mathsf{ID}_{\mathcal{T}_j}\}$	–
$D15$	$A12$	$R1$	$\mathsf{CD}\vert \equiv \phi(\{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathsf{CD}}, N_{\mathcal{T}_{j,2}}, \mathsf{ID}_{\mathcal{T}_j}\})$	–
$D16$	$IM7$, $A27$,$A17$,$D15$,$D14$	$I1$	$\mathsf{CD}\vert \equiv \mathcal{T}_j\vert \sim \{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathsf{CD}}, N_{\mathcal{T}_{j,2}}, \mathsf{ID}_{\mathcal{T}_j}\}$	–
$D17$	$D16$	$I7$	$\mathsf{CD}\vert \equiv \mathcal{T}_j\vert \sim N_{\mathcal{T}_{j,2}}$	$G6$
$D18$	$IM7$, $A27$,$A17$,$D15$,$D14$	$I1$	$\mathsf{CD}\vert \equiv \mathcal{T}_j \ni \{\mathsf{ID}_{\mathcal{R}_i}, N_{\mathsf{CD}}, N_{\mathcal{T}_{j,2}}, \mathsf{ID}_{\mathcal{T}_j}\}$	–
$D19$	$D18$	$P3$	$\mathsf{CD}\vert \equiv \mathcal{T}_j \ni N_{\mathsf{CD}}$	$G7$

2) THE SCYTHER TOOL PROOF

In this section, we evaluate the security of ISMAP using the Scyther tool. It is an automatic tool for checking the security or insecurity of protocols which is written in Python language. To evaluate the security of protocol using the Scyther tool, the following steps should be performed:

- expressing the desired protocol in the Security Protocol Description Language (SPDL);
- expressing security claims in the protocol specifications;
- performing the necessary settings, such as maximum number of runs, determining search pruning and maximum number of patterns per claim in the Scyther tool's settings;
- running the code of protocol and getting the result. If the Scyther tool can not find the attack, it evaluates the security feature OK, and if it succeeds in finding the attack, it fails that feature and shows the flowchart of the attack scenario.

For security analysis, ISMAP was described in the Security Protocol Description Language (SPDL) as it is described in Figure 3. Figure 4 depicts the results of security verification of ISMAP in the Scyther tool, which confirms the security of ISMAP.

VI. CONCLUSIONS

In this article, we analyzed the security of a mutual authentication protocol proposed by Wang and Ma. Our security analysis shows critical security flaws in this scheme, which were missed by the protocol designers and previous studies also. By exploiting these pitfalls, an active adversary ($\mathcal{A}$) who has already compromised some RFID tags may successfully impersonate an RFID reader ($\mathcal{R}_i$) or the central database (CD) or server. Finally, we introduced an adversary model that takes into account that the communication channel between an RFID reader and the database server is insecure. Furthermore, we introduced an improved server-mounted protocol, called ISMAP and showed that ISMAP provides desired security against various attacks, include the new attack that has been introduced in this paper.

However, in this paper we have not considered multi-server or multi-reader environments [49], [50]. Given that, in ISMAP, we have embedded a counter on the reader and the counter value is updated, it could be a source of desynchronization attack in such environments. Hence, assuming any tag can communicate with any reader/server, designing a secure protocol for multi-server/reader environments is an interesting challenge which we leave it as future work.

ACKNOWLEDGEMENT

The authors gratefully thank all the anonymous reviewers for their valuable comments which helped us to improve the technical content and presentation of the work significantly. They also would like to thank Pedro Peris-Lopez and Aikaterini Mitrokotsa for their invaluable helps and discussions through this work. The paper was created with using institutional support for long-term conceptual development of research organization University of Finance and Administration.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2] *Disruptive Civil Technologies. Six Technologies With Potential Impacts on us Interests Out to 2025*, Nat. Intell. Council, Washington, DC, USA, Apr. 2008. [Online]. Available: https://www.hsdl.org/?view&did=485606

[3] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for Internet of Things: A comprehensive survey," *Secur. Commun. Netw.*, vol. 2017, Aug. 2017, Art. no. 6562953.

[4] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of Things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios," *IEEE Access*, vol. 8, pp. 23022–23040, 2020.

[5] I. Markit. *Number of Connected IoT Devices Will Surge to 125 Billion by 2030*. Accessed:Mar. 29, 2020. [Online]. Available: https://technology.informa.com/596542

[6] I. Markit, *The Internet of Things: A movement, not a market*. Accessed: Mar. 23, 2020. [Online]. Available: https://cdn.ihs.com/www/pdf/IoT_ebook.pdf

[7] *Internet of Things Market Analysis 2026*. Accessed: Mar. 23, 2020. [Online]. Available: https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307

[8] M. Presser and A. Gluhak, "The Internet of Things: Connecting the real," in *World With the Digital World, The Magazine for Telecom Insiders*, vol. 2. Heidelberg, Germany: Eurescom GmbH, 2009.

[9] L. Xiao, H. Xu, F. Zhu, R. Wang, and P. Li, "SKINNY-based RFID lightweight authentication protocol," *Sensors*, vol. 20, no. 5, p. 1366, Mar. 2020.

[10] Z. Shi, X. Zhang, and J. Liu, "The lightweight RFID grouping-proof protocols with identity authentication and forward security," *Wireless Commun. Mobile Comput.*, vol. 2020, Oct. 2020, Art. no. 8436917.

[11] P. K. Maurya and S. Bagchi, "Cyclic group based mutual authentication protocol for RFID system," *Wireless Netw.*, vol. 26, no. 2, pp. 1005–1015, Feb. 2020.

[12] J. Lu, D. Liu, H. Li, C. Zhang, and X. Zou, "A fully integrated HF RFID tag chip with LFSR-based light-weight tripling mutual authentication protocol," *IEEE Access*, vol. 7, pp. 73285–73294, 2019.

[13] M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura, and J. H. Khor, "Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains," *IEEE Access*, vol. 7, pp. 7273–7285, 2019.

[14] R. Baashirah and A. Abuzneid, "Survey on prominent RFID authentication protocols for passive tags," *Sensors*, vol. 18, no. 10, p. 3584, Oct. 2018.

[15] M. Xiao, W. Li, X. Zhong, K. Yang, and J. Chen, "Formal analysis and improvement on ultralightweight mutual AuthenticationProtocols of RFID," *Chin. J. Electron.*, vol. 28, no. 5, pp. 1025–1032, Sep. 2019.

[16] M. Safkhani and N. Bagheri, "Generalized desynchronization attack on UMAP: Application to rcia, kmap, SLAP and sasi$^+$ protocols," *IACR Cryptol. Arch.*, vol. 2016, p. 905, Oct. 2016.

[17] C.-T. Li, C.-Y. Weng, and C.-C. Lee, "A secure RFID tag authentication protocol with privacy preserving in telecare medicine information system," *J. Med. Syst.*, vol. 39, no. 8, p. 77, Aug. 2015.

[18] S. Han, T. Dillon, and E. Chang, "Anonymous mutual authentication protocol for RFID tag without back-end database," in *Proc. 3rd Int. Conf., Mobile Ad-Hoc Sensor Netw.*, in Lecture Notes in Computer Science, vol. 4864. Beijing, China: Springer, Dec. 2007, pp. 623–632.

[19] C. Tan, B. Sheng, and Q. Li, "Secure and serverless RFID authentication and search protocols," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1400–1407, Apr. 2008.

[20] B. Wang and M. Ma, "A server independent authentication scheme for RFID systems," *IEEE Trans. Ind. Informat.*, vol. 8, no. 3, pp. 689–696, Aug. 2012.

[21] P. Huang, H. Mu, and F. Zeng, "Analysis on the performance of server-less RFID searching protocol," *CIT*, vol. 23, no. 4, pp. 295–302, 2015.

[22] J. Li, Z. Zhou, and P. Wang, "Server-less lightweight authentication protocol for RFID system," in *Proc. 3rd Int. Conf.*, vol. 10603, X. Sun, H. Chao, X. You, and E. Bertino, Eds. Nanjing, China: Springer, Jun. 2017, pp. 305–314.

[23] S. Sundaresan, R. Doss, S. Piramuthu, and W. Zhou, "A secure search protocol for low cost passive RFID tags," *Comput. Netw.*, vol. 122, pp. 70–82, Jul. 2017.
[24] C.-G. Liu, I.-H. Liu, C.-D. Lin, and J.-S. Li, "A novel tag searching protocol with time efficiency and searching accuracy in RFID systems," *Comput. Netw.*, vol. 150, pp. 201–216, Feb. 2019.
[25] C. Yang, C. Lee, and S. Hsiao, "Man-in-the-middle attack on the authentication of the user from the remote autonomous object," *I. J. Netw. Secur.*, vol. 1, no. 2, pp. 81–83, 2005.
[26] L. Gao, L. Zhang, F. Lin, and M. Ma, "Secure RFID authentication schemes based on security analysis and improvements of the USI protocol," *IEEE Access*, vol. 7, pp. 8376–8384, 2019.
[27] J. Guo, T. Peyrin, and A. Poschmann, "The PHOTON family of lightweight hash functions," in *Proc. 31st Annu. Cryptol. Conf.*, vol. 6841, P. Rogaway, Ed. Santa Barbara, CA, USA: Springer, 20110, 2011, pp. 222–239.
[28] J.-P. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia, "Quark: A lightweight hash," *J. Cryptol.*, vol. 26, no. 2, pp. 313–339, Apr. 2013.
[29] T.-L. Lim, T. Li, and T. Gu, "Secure RFID identification and authentication with triggered hash chain variants," in *Proc. 14th IEEE Int. Conf. Parallel Distrib. Syst.*, Dec. 2008, pp. 583–590.
[30] T. van Deursen, "50 ways to break RFID privacy," in *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*. Helsingborg, Sweden: Springer, Aug. 2010, pp. 192–205.
[31] G. P. Hancke, "Practical attacks on proximity identification systems," in *Proc. IEEE Symp. Secur. Privacy*, Oct. 2006, pp. 328–333.
[32] I. Coisel and T. Martin, "Untangling RFID privacy models," *J. Comput. Netw. Commun.*, vol. 2013, pp. 1–26, Oct. 2013.
[33] M. E. Namin, M. Hosseinzadeh, N. Bagheri, and A. Khademzadeh, "RSPAE: RFID Search Protocol based on Authenticated Encryption," *J. Electr. Comput. Eng. Innov.*, vol. 6, no. 2, pp. 179–192, 2018.
[34] M. Eslamnezhad Namin, M. Hosseinzadeh, N. Bagheri, and A. Khademzadeh, "A secure search protocol for lightweight and low-cost RFID systems," *Telecommun. Syst.*, vol. 67, no. 4, pp. 539–552, Apr. 2018.
[35] M. Safkhani, "On the security of tan serverless RFID authentication and search protocols," in *Proc. 8th Int. Workshop*, vol. 7739, J. Hoepman and I. Verbauwhede, Eds. Nijmegen, The Netherlands: Springer, 2012, pp. 1–19.
[36] L. Gong, R. Needham, and R. Yahalom, "Reasoning about belief in cryptographic protocols," in *Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy*, 1990, pp. 234–248.
[37] P. Syverson and I. Cervesato, "The logic of authentication protocols," in *Proc. Int. School Found. Secur. Anal. Des. (FOSAD)*. Bertinoro, Italy: Springer, Sep. 2000, pp. 63–137.
[38] M. Burrows, M. Abadi, and R. Needham, "BAN a logic of authentication," in *Proc. IEEE Symp. Secur. Privacy (S P)*, Oakland, CA, USA, May 2008.
[39] A. Armando, "The AVISPA tool for the automated validation of Internet security protocols and applications," in *Proc. 17th, Int. Conf. Comput. Aided Verification (CAV)*. Edinburgh, U.K: Springer, Jul. 2005, pp. 281–285.
[40] B. Blanchet and A. Chaudhuri, "Automated formal analysis of a protocol for secure file sharing on untrusted storage," in *Proc. IEEE Symp. Secur. Privacy*, May 2008, pp. 417–431.
[41] B. Blanchet, "CryptoVerif: Computationally sound mechanized prover for cryptographic protocols," in *Dagstuhl Seminar Formal Protocol Verification Appl.*, p. 117, p. 156, Oct. 2007.
[42] C. J. F. Cremers, "The Scyther tool: Verification, falsification, and analysis of security protocols," in *Computer Aided Verification* Berlin, Germany: Springer, 2008, pp. 414–418.
[43] H. Liu, X. Yao, T. Yang, and H. Ning, "Cooperative privacy preservation for wearable devices in hybrid computing-based smart health," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1352–1362, Apr. 2019.
[44] C.-I. Fan and Y.-H. Lin, "Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 933–945, Dec. 2009.
[45] J. Cao, M. Ma, Y. Fu, H. Li, and Y. Zhang, "CPPHA: Capability-based privacy-protection handover authentication mechanism for SDN-based 5G HetNets," *IEEE Trans. Dependable Secure Comput.*, early access, May 14, 2019, doi: 10.1109/TDSC.2019.2916593.
[46] M. Safkhani and A. Vasilakos, "A new secure authentication protocol for telecare medicine information system and smart campus," *IEEE Access*, vol. 7, pp. 23514–23526, 2019.
[47] R. Amin, P. Lohani, M. Ekka, S. Chourasia, and S. Vollala, "An enhanced anonymity resilience security protocol for vehicular ad-hoc network with scyther simulation," *Comput. Electr. Eng.*, vol. 82, Mar. 2020, Art. no. 106554.
[48] Y. Ma, L. Yan, X. Huang, M. Ma, and D. Li, "DTLShps: SDN-based DTLS handshake protocol simplification for IoT," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3349–3362, Apr. 2020.
[49] C.-T. Chen and C.-C. Lee, "A two-factor authentication scheme with anonymity for multi-server environments," *Secur. Commun. Netw.*, vol. 8, no. 8, pp. 1608–1625, May 2015.
[50] J. Zhao, W. Bian, D. Xu, B. Jie, X. Ding, W. Zhou, and H. Zhang, "A secure biometrics and PUFs-based authentication scheme with key agreement for multi-server environments," *IEEE Access*, vol. 8, pp. 45292–45303, 2020.

MEHDI HOSSEINZADEH received the B.S. degree in computer hardware engineering from Islamic Azad University, Dezfol Branch, Iran, in 2003, and the M.Sc. and Ph.D. degrees in computer system architecture from the Science and Research Branch, Islamic Azad University, Tehran, Iran, in 2005 and 2008, respectively. He is currently an Associate Professor with the Iran University of Medical Sciences (IUMS), Tehran. He is the author/coauthor of more than 120 publications in technical journals and conferences. His research interests include SDN, information technology, data mining, big data analytics, E-commerce, E-marketing, and social networks.

JAN LANSKY received the M.S. and Ph.D. degrees in computer science: software systems from Charles University, Prague, Czech Republic, in 2005 and 2009, respectively. He has been a Professor with the Department of Computer Science and Mathematics, Faculty of Economic Studies, University of Finance and Administration, Prague, since March 2009, where he has been the Head of the Department, since September 2014. His research interests include cryptocurrencies, text compression, and databases.

AMIR MASOUD RAHMANI received the B.S. degree in computer engineering from Amir Kabir University, Tehran, in 1996, the M.S. degree in computer engineering from the Sharif University of Technology, Tehran, in 1998, and the Ph.D. degree in computer engineering from IAU University, Tehran, in 2005. He is currently a Professor with the Department of Computer Engineering, IAU University. He is the author/co-author of more than 200 publications in technical journals and conferences. His research interests are in the areas of distributed systems, the Internet of Things, and evolutionary computing.

CUONG TRINH received the M.Sc. degree in computer science from Military Technical Academy, Vietnam, in 2014. He is currently pursuing the Ph.D. degree in informatics, communication technology, and applied mathematics with the Technical University of Ostrava, Czech Republic. His research interests include data mining, parallel computing, network infrastructure, and network security. He has a lot of experience in system network deployment, implemented RFID applications for some fields such as a library, education, and transportation systems.

MASOUMEH SAFKHANI received the Ph.D. degree in electrical engineering from the Iran University of Science and Technology, in 2012, majoring in the security analysis of RFID protocols. She is currently an Assistant Professor with the Computer Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran. Her current research interests include the security analysis of lightweight and ultralightweight protocols, targeting constrained environments, such as RFID, the IoT, VANET, and WSN. She is the author/coauthor of over 50 technical articles in information security and cryptology in major international journals and conferences.

NASOUR BAGHERI received the M.S. and Ph.D. degrees in electrical engineering from the Iran University of Science and Technology (IUST), Tehran, Iran, in 2002 and 2010, respectively. He is currently an Associate Professor with the Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran. He is also a part-time Researcher with the Institute for Research in Fundamental Sciences. He is the author of more than 100 articles in information security and cryptology. His research interests include cryptology, more precisely, designing and analysis of symmetric schemes, such as lightweight ciphers, i.e., block ciphers, hash functions, and authenticated encryption schemes, cryptographic protocols for the constrained environment, such as RFID tags and the IoT edge devices and hardware security, i.e., the security of symmetric schemes against side-channel attacks, such as fault injection and power analysis.

BAO HUYNH received the M.Sc. degree in computer science from the Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam, in 2011, and the Ph.D. degree in computer science from the VSB—Technical University of Ostrava, Czech Republic, in 2017. Since then, he continuously researched and developed new algorithms that are helpful for real applications in various fields. His research interests include data mining, privacy-preserving, big data analytics, parallel computing, social networks, network infrastructure, and network security. In addition, he has over ten years of experience in design, and implements network infrastructure systems and security network system.