Digital Communications and Networks 9 (2023) 710–716

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

Secure ticket-based authentication method for IoT applications

Mojtaba Alizadeh [a], Mohammad Hesam Tadayon [b,*], Alireza Jolfaei [c]

[a] Computer Engineering Department, Lorestan University, Khorramabad, Iran
[b] Iran Telecommunication Research Center (ITRC), Tehran, Iran
[c] Department of Computing, Macquarie University, Sydney, Australia

ARTICLE INFO

Keywords:
IoT
Internet of things
Authentication
Privacy
Security

ABSTRACT

The recent surge in the number of machines, appliances, and services connected to the Internet demands secure processing and transmission of sensory data. Authentication plays a crucial role in a typical security model used in the Internet of Things (IoT), and it protects data communications from various attacks, such as impersonation and denial of service, by verifying and allowing legitimate users to access the IoT resources. However, recent authentication literature has not addressed the need for developing a scalable and efficient authentication method in this field. This paper proposes a secure and anonymous ticket-based authentication method for the IoT. The proposed method protects the network from various security and privacy threats such as data alternation and denial of service while also offering mutual authentication and sensor anonymity. Our security and performance evaluations confirm the improvement.

1. Introduction

The number of mobile devices connected to the Internet is increasing tremendously, necessitating seamless connectivity for wireless communication environments. As part of this network communication, Internet of Things (IoT) technology provides a seamless connection to billions of intelligent machines, objects, and sensors [1]. IoT was introduced in the early 2000s by Kevin Ashton, a member of the MIT Auto-ID Center, referring to the binding of information from the Radio Frequency Identifiers (RFIDs) to the Internet [2]. Shortly afterwards, the attention given to the Internet of related objects by top IT organizations and governments increased as they realized that this concept could be a major driver of future economic development and sustainability. For example, the International Telecommunication Union (ITU) published the "ITU Internet Report 2005: Internet of Things (IoT)" and formally introduced the concept of the IoT. Subsequently, the European Union issued a Commission Communication on RFID to adopt this IoT concept in March 2007 [3].

The IoT links objects with Internet capabilities using the equipment that can sense and exchange communication information to gain the intellectualized ability to complete various tasks, such as identifying, positioning, and monitoring [4]. It was estimated by Cisco that the IoT would expand to approximately 50 billion units installed by 2020. Several of its most critical applications would be in the areas of e-health, assisted living, enhanced learning, and home automation [5].

Currently, there are two unique trends for IoT development. First, the smart dust movement, which promotes tiny and inexpensive devices that include RFID chips [6,7]; second, the Web of Things (WoT), which intends to link extra powerfully embedded devices with IoT using Web protocols instead of using lower network layers communication [8]. This study focuses on the field of Wireless Sensor Networks (WSN) that refers to a particular IoT subset and reveals characteristics of both movements. Fig. 1 illustrates the key concepts and technology behind the categorized standards that represent the IoT.

The rest of this paper is organized as follows:

Section 2 discusses previous literature, and Section 3 explains the details of the proposed method. Section 4 provides a security analysis, and Section 5 offers a formal security analysis using Burrows–Abadi–Needham (BAN) logic. Section 6 offers a complexity analysis, and Section 7 concludes the research.

2. Literature review

Combining this case's heterogeneity with the IoT's large-scale systems will possibly increase the magnitude of current Internet security attacks because it is currently used for interactions between humans, robots, machines, and combinations thereof. Specifically, some conventional security countermeasures and privacy controls cannot be directly applied

* Corresponding author.
E-mail addresses: alizadeh.mo@lu.ac.ir (M. Alizadeh), tadayon@itrc.ac.ir (M.H. Tadayon), alireza.jolfaei@mq.edu.au (A. Jolfaei).

https://doi.org/10.1016/j.dcan.2021.11.003
Received 8 September 2020; Received in revised form 13 September 2021; Accepted 15 November 2021
Available online 23 November 2021

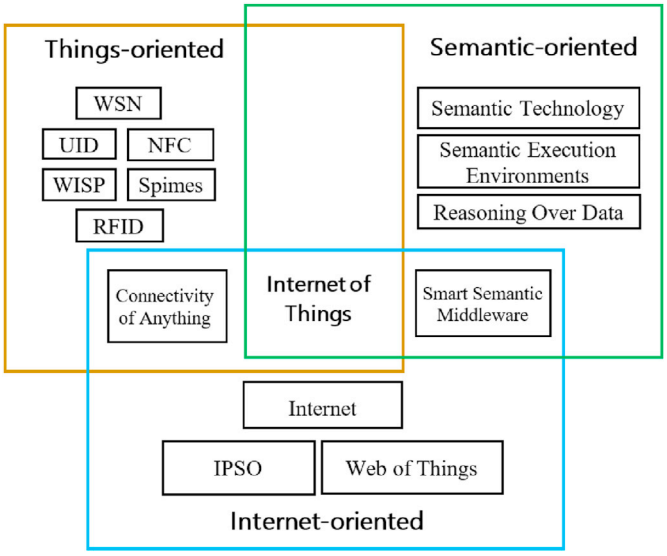

Fig. 1. Convergence model of various IoT model perspectives [9].

to IoT technology because of its computing power constraints [10]; the large number of interlinked devices introduces scalability challenges. Meanwhile, to gain full trust, valid sensor, security, trust, and privacy models must be described in an IoT application context [11]. Data security, confidentiality, integrity, and anonymity must be guaranteed, which requires authorization and authentication techniques [12,13]. Regarding privacy requirements, personal information and sensor data must be protected, and confidentiality must be guaranteed because the compromising of either could reveal sensitive information (e.g., sensor habits) [14]. Trust is a basic aspect as the IoT environment is marked by various devices that process and manage data in compliance with sensor rights and requirements. Self-healing and adaptation have major roles in IoT infrastructure, addressing standard and unanticipated changes in the targeted environment. Along with traditional security methods, devices also require built-in or embedded security systems installed for robust prevention, detection, isolation, and diagnosis, as well as countermeasures for fighting successful breaches [15].

Security design starts with selecting the credentials that will be utilized by IoT devices to achieve network access authorization and subsequent application requests. Well-known industry standards include ID/password pairs, SIM cards, and certificates [16]. Each of these credentialing options has benefits and drawbacks. For example, ID/password pairs are comparatively lightweight yet cannot be managed practically in large amounts. Although beneficial, SIM cards can only be applied to small group distribution due to the implementation cost. Certificates offer dynamic and mature solutions for large-scale applications, yet vendors seeking certificate authority (CA) must incur additional costs.

Device selection can also determine the associated credential. While ID/password pairs can be supplied by manufacturers to service providers for device management, certificates allow service providers to overwrite them [17]. In addition, devices that change service providers might need a re-provisioning process that could also affect credential selection. For instance, credentials based on ID/password pairs may not remain identical when a device is transferred to another provider in multi-provider roaming IoT SIM cards. Agreeing on one credential type for all applications and devices is difficult for the industry [18].

The IoT is projected to face fragmentation just like the Internet, making application profiling necessary to improve interoperability and prevent such a possibility. Notably, discovering a secure service provider and a service-specific supplier is extremely challenging. Device-initiated and selection mechanism discoveries face insufficient human sensors and a large number of devices with complex preconfigurations. Furthermore, discoveries initiated by network and mechanism selection cause problems with ownership because devices on the IoT would have difficulty becoming aware of their own accessible state by specific service providers. It is already difficult to manage one set of credentials; Considering separate and applicable network access services, it is more difficult to manage multiple credentials. Thus, it is tough to utilize similar credentials for both kinds of access. Moreover, single sign-on methods have been considered as extra optimization techniques. Devices using the IoT are projected to become pervasive in daily living [10]. Sensor activity requires close monitoring and reporting, without which human privacy can be endangered. Such concerns make hiding device identifiers from the elements and neighboring intermediaries crucial [14].

Table 1
Notations of the proposed scheme.

Symbol	Description
GWN	Gateway
SN	Sensor
x	The AAA secret key
R_i	Random number of entity (i)
ID_{SN}	Sensor identification
ID_G	Gateway identification
PW_{SN}	Sensor password
SK_{i-j}	entity(i) and entity(j) session key
$E_{SK_{i-j}}(M)$	M is encrypted by SK_{i-j}
N_i	Nonce of entity(i)
$E_K(M)$	M is encrypted by key, K
$h(\cdot)$	Hash function (one-way)
SGA	Symmetric key shared with all nodes
$\|$	Concatenation
$\oplus$	XOR operation

The literature indicates a need for a secure and anonymous IoT authentication mechanism, which has prompted the authentication method proposed by this research. Atzori et al. [5] surveyed related challenges of the IoT paradigm and analyzed IoT's enabling technologies as well as other middleware using an application perspective. Through this, they discussed privacy, security, standardization, management, and networking issues. They concluded that current technologies do not cover the IoT scalability and efficiency requirement. Ref. [19] focused on major research contexts (e.g., activity and project standardization as well as affected areas) that included challenges in managing data privacy, confidentiality, and trust in relation to IoT security needs. Ref. [20] discussed the challenges of privacy and security issues based on a legislative perspective specifically related to the directives given by the European Commission. Ref. [21] discussed the Internet of Underwater Things and provided direction for dealing with security issues such as vulnerabilities to malicious attacks and self-protection. Ref. [22] examined distributed and centralized architectural benefits and drawbacks from the perspective of IoT privacy and security, analyzing attack models and threats. Ref. [9] offered an overall view of different IoT aspects (including involved technologies, applications, and architectures) while also discussing cloud platforms, energy consumption, security, service quality, and data mining implications. The stated open challenges of this study inspired us to propose a suitable authentication method for the IoT. Finally, Ref. [3,23] focused on IoT trust management and authentication in specific.

This study focuses on object authentication solutions for an IoT environment. Some ideas were drawn from our previous study of Proxy Mobile IPv6 (PMIPv6) networks [24]. The proposed method is based on applying disposable ticketing during authentication. To achieve a high level of security, gateway and IoT nodes are mutually authenticated.

3. Proposed scheme

The proposed authentication method is explained in this section. The novelty of the proposed method is providing object anonymity via alias ID introduction. Furthermore, using a lightweight hash function instead

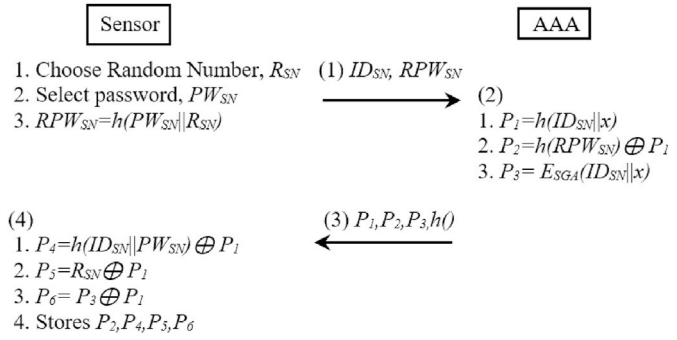

Fig. 2. Initial registration phase.

of the energy-consuming cryptographic algorithm will improve sensor performance.

The scheme comprises three phases: initial sensor registration with the authentication server, login, and authentication. We propose a method called the Ticket-based Authentication Method for IoT (TAMI). The notations of the TAMI scheme are defined in Table 1.

3.1. Assumptions

The following assumptions are used in the proposed method:

- Sensors (SNs) are not equipped with tamper-resistant smart cards; therefore, attackers can access all stored data should a node be captured.
- Gateway (GWN) is safe and secure.

3.2. Initial registration

In this phase, a sensor is registered on the authentication server (AAA) for further communication. Fig. 2 illustrates the initial authentication procedure.

3.3. Authentication phase

The mutual authentication between SN and GWN is initiated by SN. In this phase, the authentication ticket for the sensor is generated by the AAA, which can be used in other authentication procedures if SN roams within the IoT network. This anonymous ticket contains information that includes an expiry time and IoT node ID. Furthermore, mutual authentication between IoT nodes and GWN is applied in TAMI to prevent a bogus GWN attack [3]. The authentication procedure is as follows:

1. SN → GWN: MS_1

The SN is initially verified by a smart card by entering ID_{SN} and PW_{SN} into the smart card. The smart card then initiates the following procedure to check sensor authenticity:

a) $h(ID_{SN} \| PW_{SN})$ *b)* $P_1 \leftarrow h(ID_{SN} \| PW_{SN}) \oplus P_4$ *c)* $R_{SN} \leftarrow P_1 \oplus P_5$ *d)* $RPW_{SN} \leftarrow h(R_{SN} \| PW_{SN})$ *e)* $P_2 = ?\ h(RPW_{SN}) \oplus P_1$

If ID_{SN} and PW_{SN} are valid, SN generates a random number, $a^i, N_U^i = a^i$ G mod n, and calculates SN alias ID, $AID_{SN} = ID_{SN} \oplus h(P_1 \| N_{SN}^i)$ to preserve SN anonymity. In addition, it calculates $E_{P_1}(h(P_1 \| N_{SN}^i) \| N_{SN}^i)$, and $P_3 = P_6 \oplus P_1 = P_6 \oplus P_5 \oplus R_{SN}$. Finally, it generates the message, MS_1 : $(AID_{SN} \| P_3 \| E_{P_1}(h(P_1 \| N_{SN}^i) \| N_{SN}^i))$ and sends it to the GWN.

2. GWN → AAA: $(MS_1 \| E_{P_1}(ID_{GWN} \| N_{GWN}^i \| T_1))$

The GWN decodes $P_3 = E_{SGA}(ID_{SN} \| x)$ using the shared key, SGA, to obtain ID_{SN} and secret x. Then, the GWN calculates $P_1 = h(ID_{SN} \| x)$ to decrypt $E_{P_1}(h(P_1 \| N_{SN}^i) \| N_{SN}^i)$ and find SN nonce, N_{SN}^i. If the received value $h(P_1 \| N_{SN}^i)$ is equal to the value received by the GWN, the IoT SN is authenticated. After the SN authentication process, the GWN proceeds to calculate b^i, $N_{GWN}^i = b^i G$ mod n. At the last step, GWN calculate $E_{P_1}(ID_{GWN} \| N_{GWN}^i \| T_1)$, which is used as a message with time stamp T_1. Finally, the GWN sends $MS_1 \| E_{P_1}(ID_{GWN} \| N_{GWN}^i \| T_1)$ to AAA.

3. AAA → GWN: $(AM_1 \| E_{P_1}(AM_2 \| c^i N_{SN}^i \| T_3 \| TIK \| K_{TK}))$

The AAA computes $P_1 = h(ID_{SN} \| x)$, then it decrypts $E_{P_1}(ID_{GWN} \| N_{GWN}^i \| T_1)$ using its key, P_1, to obtain T_1 and the GWN nonce. Afterwards, it checks if the message is fresh by calculating $T_2 - T_1 \leqslant \Delta T$. Then, it selects a random number, c^i, to calculate $c^i N_{GWN}^i = c^i b^i G$ mod n and $c^i N_{SN}^i = c^i a^i G$ mod n, and decrypts $MS1$ using key $P_1 = h(ID_{SN} \| x)$. The AAA then calculates two values, $AM_1 = h(ID_{AAA} \| x) \oplus N_{SN}^i \oplus c^i N_{GWN}^i$, and $AM_2 = h(ID_{AAA} \| x) \oplus c^i N_{SN}^i \oplus c^i N_{GWN}^i$ before issuing a ticket $TIK = E_{K_{TIK}}(AID_{SN} \| T_{EX})$, where T_{EX} is the ticket expiration time. Finally, AAA sends the message, $(AM_1 \| E_{P_1}(AM_2 \| c^i N_{SN}^i \| T_3 \| TIK \| K_{TIK})$, to the gateway node, where T_3 is time stamp.

4. GWN → SN: $(AM_1 \| E_{SK_{GWN-SN}^i}(AM_2 \| TIK))$

The GWN node decrypts $E_{P_1}(AM_2 \| c^i N_{SN}^i \| T_3 \| TIK \| K_{TIK})$ and checks the freshness of the message T_3. Then, the node calculates a session key between the GWN and sensor, $SK_{GWN-SN}^i = b^i c^i N_{SN}^i = b^i c^i a^i G$ mod n, and encrypts $(AM_2 \| TIK)$. Finally, it sends $(AM_1 \| E_{SK_{GWN-SN}^i}(AM_2 \| TIK))$ to the SN.

5. SN → GWN: $E_{SK_{GWN-SN}^i}(TIK \| T_4)$

The SN computes $(c^i N_{GWN}^i = h(ID_{AAA} \| x) \oplus N_{SN}^i \oplus AM_1)$, and then calculates the session key, $SK_{GWN-SN}^i = a^i c^i N_{GWN}^i = a^i c^i b^i G$ mod n, to obtain TIK and AM_2 by decrypting $E_{SK_{GWN-SN}^i}(AM_2 \| TIK)$. At this point, the SN can

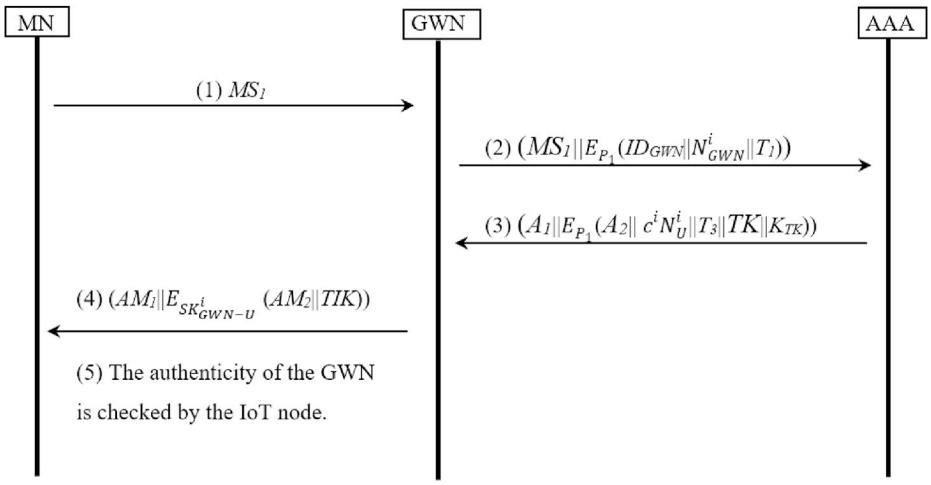

Fig. 3. TAMI login phase.

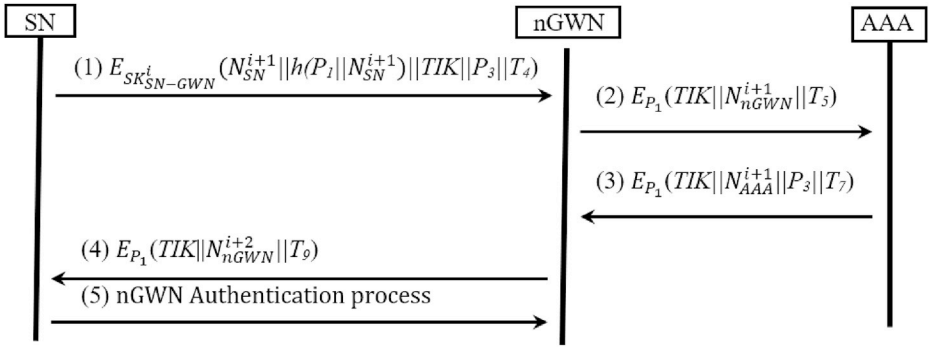

Fig. 4. Handover authentication phase of TAMI.

mutually check the GWN authenticity by comparing the result of value $AM_2 = h(ID_{AAA}||x) \oplus c^i N^i_{SN} \oplus c^i N^i_{GWN}$ to the received AM_2; if both values are equal, the GWN is a legitimate entity. Finally, the SN encrypts $(TIK||T_4)$ using SK^i_{GWN-SN} and sends it to the GWN.

The GWN decrypts $E_{SK^i_{GWN-SN}}(TIK||T_4)$ and checks the message freshness. At this point, the mutual authentication between the GWN and the SN is completed and the SN is permitted to access the IoT network. The authentication phase process is illustrated in Fig. 3.

3.4. Handover authentication

An SN can roam inside an IoT network and connect to any gateway. During the handover from the previous gateway (*pGWN*) and new gateway (*nGWN*), an SN should be authenticated again, using TIK as its authenticity credentials. The session key between the SN and the pGWN, SK^i_{GWN-SN} is assumed to be transferred to the new gateway using a secure channel. The handover procedure is as follows:

1. SN → nGWN: $E_{SK^i_{SN-GWN}}(N^{i+1}_{SN}||h(P_1||N^{i+1}_{SN}))||TIK||P_3||T_4)$

First, the SN generates its nonce, N^{i+1}_{SN}, and $h(P_1 \oplus N^{i+1}_{SN})$. Then, using session key SK^i_{SN-GWN}, it encrypts $(N^{i+1}_{SN} \oplus TIK)$ using stored ticket, *TIK*, and sends $E_{SK^i_{SN-GWN}}(N^{i+1}_{SN}||h(P_1 \oplus N^{i+1}_{SN}) \oplus TIK \oplus P_3 \oplus T_4)$ to the nGWN.

2. nGWN → AAA: $E_{P_1}(TIK||h(P_1||N^i_{SN}))||N^{i+1}_{nGWN}||T_5)$

The nGWN decrypts $E_{SK^i_{SN-GWN}}(N^{i+1}_{SN}||h(P_1||N^{i+1}_{SN}))||TIK||P_3||T_4)$ to obtain P_3. Using the shared secret key, *SGA*, it decrypts P_3 to find ID_{SN} and value x. Message freshness is then checked by calculating $T_5 - T_4 \leqslant \Delta T$. Using the received SN nonce, N^{i+1}_{SN}, the nGWN calculates $P_1 = h(ID_{SN}||x)$ and $h(P_1||N^i_{SN})$; if the received value is equal to the value received by the nGWN, the IoT SN is considered to be authenticated. Finally, the nGWN sends $E_{P_1}(TIK||h(P_1||N^i_{SN}||N^{i+1}_{nGWN}||T_5)$ to the AAA.

3. AAA → nGWN: $E_{P_1}(TIK||N^{i+1}_{AAA}||P_3||T_7)$

The AAA computes $P_1 = h(ID_{SN}||x)$, then decrypts $E_{P_1}(TIK||h(P_1||N^i_{SN})||N^{i+1}_{nGWN}||T_5)$ using its key, P_1, to obtain nGWN nonce and *TIK*. Message freshness is subsequently checked by calculating $T_6 - T_5 \leqslant \Delta T$. The AAA proceeds to check the ticket expiry time, T_{EX}, obtained by decrypting *TIK* using the key, K_{TIK}. If the ticket is still valid, the AAA sends back $E_{P_1}(TIK||N^{i+1}_{AAA}||P_3||T_7)$ to nGWN.

4. nGWN → SN: $E_{P_1}(TIK||N^{i+2}_{nGWN}||T_9)$

The nGWN decrypts $E_{P_1}(TIK||N^{i+1}_{AAA}||P_3||T_7)$, and checks the message freshness by calculating $T_8 - T_7 \leqslant \Delta T$. Then, it decrypts P_3 to find ID_{SN} and x, using these two values, it calculates P_1. Finally, the nGWN encrypts $(TIK||N^{i+2}_{nGWN}||T_9)$ using P_1 and sends it to the SN.

5. nGWN authentication process.

The SN decrypts $E_{P_1}(TIK||N^{i+2}_{nGWN}||T_9)$ using P_1, and then checks the received message freshness by calculating $T_{10} - T_9 \leqslant \Delta T$. Finally, it checks the received value, *TIK*, against the stored value; if both *TIK* are equal, then the new gateway is also authenticated. At this point, the mutual authentication between the SN and the nGWN is accomplished. Fig. 4 shows the TAMI handover procedure.

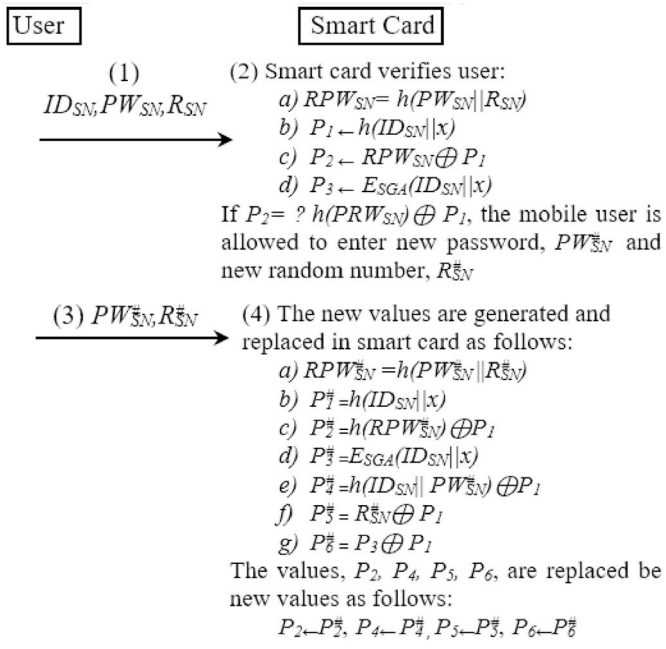

Fig. 5. Password change procedure.

3.5. Password change procedure

PW_{SN} should be changed whenever an SN requests change a new password. This procedure is explained in Fig. 5, in which # represents the new value.

4. Security analysis

In this section, the security and privacy of the proposed method are discussed based on common security theorems.

Table 2 summarizes the security solutions provided by the proposed method.

Table 2
Security criteria provided by TAMI.

Security Criteria	TAMI
Resistant to Denial-of-Service Attack	✓
Mutual Authentication	✓
Resistant to Replay Attack	✓
Sensor Anonymity	✓
Resistant to Entity Impersonation Attack	✓
Resistant to Password Guessing Attack	✓
Resistant to Forgery Attack	✓

4.1. Mutual authentication

Mutual authentication is a key security consideration for authenticating any entity, and it is applied in the proposed method. As an important procedure, both the IoT node and GWN should be authenticated to protect the IoT network against impersonation attacks. As described in Fig. 3, the GWN checks the SN's authenticity first with the help from the AAA, and then the SN checks the GWN's legitimacy. The authentication procedure will be rejected if any entity cannot be authenticated to the other during this mutual authentication mechanism.

4.2. Sensor anonymity

The anonymity of each IoT entity is preserved during authentication to protect its privacy. The privacy of each node in an IoT environment is a critical factor because an attacker can sniff signal communication, determine the identity of a node, and also analyze all received information related to that node. In the proposed method, we use alias IDs for each SN and GWN to protect anonymity. Each alias ID composes of a hashed ID, SN secret, x, and nonce, which makes any object's real ID complicated because attackers must know the object's secret to determine its real ID. Furthermore, each object ID is hashed using a one-way hash function that makes its decoding almost impossible [25].

4.3. Node and gateway impersonation attack

In the proposed method, an attacker cannot impersonate either an IoT node or a GWN because doing so requires their secrets and random numbers. Even if attackers sniff the communication signal, the actual IDs of an IoT node and GWN will be hashed using a one-way hash function.

4.4. Replay attack

In the proposed method, we add a nonce for each communication to prevent replay attacks. If attackers sniff any communication message, they cannot launch a replay attack, because the receiver checks the nonce inside the message. The receiver stops further communication procedures if the nonce is not fresh.

4.5. Forgery attack

The smart card inside the IoT node includes values P_2, P_4, P_5, P_6. If attackers access this information, they will be unable to modify any of it. For example, if attackers try to modify $P_2 = h(RPW_{SN}) \oplus P_1$, they will need the password and the random number of the SN to calculate RPW_{SN} and then $h(RPW_{SN})$, which cannot be obtained. The same will happen if an attacker tries to modify $P_4 = h(ID_{SN}||PW_{SN}) \oplus P_1$ because they will not possess the SN password and ID.

4.6. Denial-of-service attack (DoS)

A DoS attack can be launched on a GWN if an attacker sends a large number of authentication requests using a fake node. However, the proposed method prevents this from occurring. An attacker should generate $MS_1 : (AID_{SN}||P_3||E_{P_1}(h(P_1||N^i_{SN})||N^i_{SN}))$ to start a DoS attack and send it to the GWN. At this point, the attacker can either sniff the message, MS_1, and replay it to the GWN, which will reject the request after checking the nonce, or the attacker can generate message MS_1, which will fail without a ID_{SN} and a password.

4.7. Password guessing attack

An attacker must know $RPW_{SN} = h(PW_{SN}||R_{SN})$ to calculate $P_2 = h(RPW_{SN}) \oplus P_1$. Assuming the attacker can access a node smart card and obtain P_2, they will need to find $P_1 = h(ID_{SN}||x)$ to get RPW_{SN}. However, the attacker must also obtain the node's secret value and real ID, the latter of which is not used during authentication.

5. Formal security analysis

In this section, the proposed method is analyzed using common formal security analysis techniques. As common modal logic based on the reviewed literature [26–31], BAN logic [32] is used in this study.

BAN logic comprises the main phases: idealization, assumption definition, and logic rule application.

The mutual authentication between the GWN and the SN is the main goal of the proposed method. Therefore, the security objectives of the proposed method based on BAN logic are as follows:

- **Goalno.1** : $GWN \mid\equiv (SN \leftrightarrow^{SK_{SN-GWN}} GWN)$
- **Goalno.2** : $SN \mid\equiv (SN \leftrightarrow^{SK_{SN-GWN}} GWN)$
- **Goalno.3** : $SN \mid\equiv GWN \mid\equiv (SN \leftrightarrow^{SK_{SN-GWN}} GWN)$
- **Goalno.4** : $GWN \mid\equiv SN \mid\equiv (SN \leftrightarrow^{SK_{SN-GWN}} GWN)$

The next step is to transform communication messages into idealized versions. The communication messages during login phase are transformed as follows:

- M 1.1: $SN \rightarrow GWN : (SN \leftrightarrow^{h(ID_{SN}||x)} GWN, h(ID_{SN}||x), N^i_{SN}) h(ID_{SN}||x)$
- M 1.2: $SN \rightarrow GWN : (SN \leftrightarrow^{\mathrm{SGA}} GWN, ID_{SN}, x) K_{SGA}$
- M 2.1: $GWN \rightarrow AAA : (GWN \leftrightarrow^{h(ID_{SN}||x)} AAA,\ h(ID_{SN}||x),\ N^i_{SN},\ ID_{GWN},\ N^i_{GWN}, T_1) h(ID_{SN}||x)$
- M 2.2: $AAA \rightarrow GWN : (GWN \leftrightarrow^{\mathrm{SGA}} AAA, ID_{SN}, x) K_{SGA}$
- M 3.1: $GWN \rightarrow AAA : (AAA \leftrightarrow^{h(ID_{SN}||x)} GWN, AAA \leftrightarrow^{K_{TIK}} GWN, ID_{AAA}, x, c^iN^i_{SN}, c^iN^i_{GWN}, TIK, K_{TIK}, T_{EX}, T_3, AID_{SN}) h(ID_{SN}||x)$
- M 3.2: $AAA \rightarrow GWN : (GWN \leftrightarrow^{h(ID_{AAA}||x)} AAA, N^i_{SN}, c^iN^i_{GWN}) h(ID_{AAA}||x)$
- M 4.1: $GWN \rightarrow SN : (GWN \leftrightarrow^{SK_{GWN-SN}} SN,\ GWN \leftrightarrow^{K_{TIK}} SN,\ ID_{AAA},\ x, c^iN^i_{SN}, c^iN^i_{GWN}, TIK, K_{TIK}, T_{EX}, AID_{SN}) SK_{GWN-SN}$
- M 4.2: $GWN \rightarrow SN : (GWN \leftrightarrow^{h(ID_{AAA}||x)} SN, N^i_{SN}, c^iN^i_{GWN}) h(ID_{AAA}||x)$
- M 5.1: $SN \rightarrow GWN : (GWN \leftrightarrow^{SK_{GWN-SN}} SN,\ GWN \leftrightarrow^{K_{TIK}} SN,\ c^iN^i_{SN}, c^iN^i_{GWN}, T_4, TIK, K_{TIK}, T_{EX}, AID_{SN}) SK_{GWN-SN}$

The assumptions of the proposed method's authentication phase are as follows:

- A1: $SN \mid\equiv N^x_{GWN}$
- A2: $GWN \mid\equiv N^x_{SN}$
- A3: $AAA \mid\equiv N^x_{SN}$
- A4: $AAA \mid\equiv N^x_{GWN}$
- A5: $SN \mid\equiv N^x_{AAA}$
- A6: $GWN \mid\equiv N^x_{AAA}$
- A7: $SN \mid\equiv SN \leftrightarrow^{h(ID_{SN}||x)} GWN$
- A8: $GWN \mid\equiv SN \leftrightarrow^{h(ID_{SN}||x)} GWN$
- A9: $SN \mid\equiv AAA \Rightarrow (SN \leftrightarrow^{cN^{(.)}_{GWN}} GWN)$
- A10: $GWN \mid\equiv AAA \Rightarrow (SN \leftrightarrow^{cN^{(.)}_{GWN}} GWN)$
- A11: $SN \mid\equiv GWN \Rightarrow (SN \leftrightarrow^{SK_{GWN-SN}} GWN)$
- A11: $GWN \mid\equiv SN \Rightarrow (SN \leftrightarrow^{SK_{GWN-SN}} GWN)$

Based on idealized messages and the assumptions using BAN logic rules, the proposed method can be analyzed and proven as follows:

1. Based on Message 1.1 and $A8$ (message-meaning rule):

   $S1$: $GWN \mid\equiv SN \mid\sim (SN \leftrightarrow^{h(ID_{SN}||x)} GWN, h(ID_{SN}||x), N^i_{SN})$

2. Based on $S1$ and $A2$ (freshness-conjuncatenation):

$S2$: $GWN \mid\equiv SN \mid\equiv (SN \leftrightarrow^{h(ID_{SN}\|x)} GWN, h(ID_{SN}\|x), N^i_{SN})$

3. Based on $S2$ and the break conjuncatenation rule:

$S3$: $GWN \mid\equiv SN \mid\equiv (SN \leftrightarrow^{h(ID_{SN}\|x)} GWN)$

4. Based on Message 3.1 and $S3$ (message-meaning rule):

$S4$: $GWN \mid\equiv AAA \mid\sim (AAA \leftrightarrow^{h(ID_{SN}\|x)} GWN, AAA \leftrightarrow^{K_{TIK}} GWN, ID_{AAA}, x, c^iN^i_{SN}, c^iN^i_{GWN}, TIK, K_{TIK}, T_{EX}, T_3, AID_{SN})$

5. Based on $S4$ and $A6$ (freshness-conjuncatenation):

$S5$: $GWN \mid\equiv AAA \mid\equiv (AAA \leftrightarrow^{h(ID_{SN}\|x)} GWN, AAA \leftrightarrow^{K_{TIK}} GWN, ID_{AAA}, x, c^iN^i_{SN}, c^iN^i_{GWN}, TIK, K_{TIK}, T_{EX}, T_3, AID_{SN})$

6. Based on $S5$ and the break conjuncatenation rule:

$S6$: $GWN \mid\equiv AAA \mid\equiv (c^iN^i_{SN})$

7. Based on $S6$, $A10$, and the jurisdiction rule:

$S7$: $GWN \mid\equiv (c^iN^i_{SN})$

8. Based on $S7$ and $SK_{SN-GNW} = b^i(c^iN^i_{SN}) = b^ic^ia^iG$, we get:

$S8$: $GWN \mid\equiv (SN \leftrightarrow^{SK_{SN-GWN}} GWN)$ (**Goal1**)

9. Based on Message 4.2, we have:

$S9$: $SN \mid\equiv (c^iN^i_{GWN})$

10. Based on $S7$ and $SK_{SN-GNW} = b^i(c^iN^i_{SN}) = b^ic^ia^iG$, we get:

$S10$: $SN \mid\equiv (SN \leftrightarrow^{SK_{SN-GWN}} GWN)$ (**Goal2**)

11. Based on Message 4.1 and $S10$ (message-meaning rule):

$S11$: $SN \mid\equiv GWN \mid\sim (GWN \leftrightarrow^{SK_{GWN-SN}} SN,\ GWN \leftrightarrow^{K_{TIK}} SN,\ ID_{AAA},\ x, c^iN^i_{SN}, c^iN^i_{GWN}, TIK, K_{TIK}, T_{EX}, T_3, AID_{SN})$

12. Based on $S11$ and $A1$ (freshness-conjuncatenation):

$S12$: $SN \mid\equiv GWN \mid\equiv (GWN \leftrightarrow^{SK_{GWN-SN}} SN,\ GWN \leftrightarrow^{K_{TIK}} SN,\ ID_{AAA},\ x, c^iN^i_{SN}, c^iN^i_{GWN}, TIK, K_{TIK}, T_{EX}, T_3, AID_{SN})$

13. Based on $S12$ and the break conjuncatenation rule:

$S13$: $SN \mid\equiv GWN \mid\equiv (SN \leftrightarrow^{SK_{SN-GWN}} GWN)$ (**Goal3**)

14. Based on Message 5.1 and $S8$ (message-meaning rule:

$S14$: $GWN \mid\equiv SN \mid\sim (GWN \leftrightarrow^{SK_{GWN-SN}} SN,\ GWN \leftrightarrow^{K_{TIK}} SN,\ c^iN^i_{SN}, c^iN^i_{GWN}, TIK, K_{TIK}, T_{EX}, T_4, AID_{SN})$

15. Based on $S14$ and $A2$ (freshness-conjuncatenation):

$S15$: $GWN \mid\equiv SN \mid\equiv (GWN \leftrightarrow^{SK_{GWN-SN}} SN,\ GWN \leftrightarrow^{K_{TIK}} SN,\ c^iN^i_{SN}, c^iN^i_{GWN}, TIK, K_{TIK}, T_{EX}, T_4, AID_{SN})$

16. Based on $S15$ and the break conjuncatenation rule:

$S16$: $GWN \mid\equiv SN \mid\equiv (SN \leftrightarrow^{SK_{SN-GWN}} GWN)$ (**Goal4**).

Table 3
TAMI authentication scheme execution operations and phase times.

Phase	Execution Operations	Time(s)
Initial Registration	$2*T_h + 3*T_{xor} + 1*T_{rng}$	0.064075
Login	$4*T_h + 10*T_{xor} + 3*T_{cryp} + 1*T_{rng}$	0.09117
Handover	$1*T_h + 2*T_{cryp} + 1*T_{rng}$	0.08547

6. Complexity analysis

The complexity of the proposed method is analyzed in this section. When designing authentication mechanisms, the inherent processing power and storage limitations of IoT nodes must be considered. Hence, the proposed method requires fitting to the computation resources of IoT nodes. The notations used in this complexity analysis are as follows:

- T_h= Hash function execution time.
- T_{xor} = XOR operation time.
- T_{cryp} = Encryption/decryption execution time.
- T_{rng} = Random number generation time.

According to related performance analysis [33], the execution time for symmetric cryptography, random number generation, and the one-way hash function are 0.0087, 0.06307, and 0.0005 s, respectively [34]. The execution time of an *XOR* operation can be neglected because it is insignificant compared with other operations in the authentication procedure [34]. Table 3 shows the execution times for the initial registration and login phases of the proposed method.

7. Conclusions

The number of devices connected to the IoT is rapidly increasing, making IoT security an indispensable part of this technology, which can be improved by implementing an appropriate object authentication mechanism. This study proposed a secure anonymous authentication mechanism to achieve a level of security that fits the characteristics of the IoT concept. The basic idea of the proposed method is using disposable tickets during the mutual authentication of GWN and IoT nodes, preventing impersonation attacks. Node privacy is also protected via alias IDs. The security correctness of our method has been analyzed and proven using BAN logic. Finally, the results of performance analysis confirm the improvement as the proposed method uses less time-consuming cryptographic operations such as XOR operation. The proposed method provides guidance for further research on ticket-based authentication method to protect IoT.

Declaration of competing interest

There is no conflict of Interest.

References

[1] M.J. Piran, D.Y. Suh, Learning-driven Wireless Communications, towards 6G, 2019, https://doi.org/10.1109/iCCECE46942.2019.8941882. arXiv:1908.07335.
[2] S. Madakam, V. Lake, V. Lake, V. Lake, et al., Internet of things (iot): a literature review, J. Comput. Commun. 3 (2015) 164, 05.
[3] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in Internet of Things: the road ahead, Comput. Network. 76 (2015) 146–164, https://doi.org/10.1016/j.comnet.2014.11.008.
[4] P. Kumar, A. Gurtov, M. Ylianttila, S.G. Lee, H.J. Lee, A Strong Authentication Scheme with User Privacy for Wireless Sensor Networks, 2013, https://doi.org/10.4218/etrij.13.0113.0103.
[5] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Network. 54 (15) (2010) 2787–2805, https://doi.org/10.1016/j.comnet.2010.05.010.
[6] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, K.K.R. Choo, A Robust and Energy Efficient Authentication Protocol for Industrial Internet of Things, 2018, https://doi.org/10.1109/JIOT.2017.2787800.
[7] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun, K. Sakurai, Authentication in mobile cloud computing: a survey, J. Netw. Comput. Appl. 61 (2016) 59–80, https://doi.org/10.1016/j.jnca.2015.10.005.
[8] L. Qi, C. Hu, X. Zhang, M.R. Khosravi, S. Sharma, S. Pang, T. Wang, Privacy-aware data fusion and prediction with spatial-temporal context for smart city industrial environment, IEEE Trans. Ind. Inf. 17 (6) (2020) 4159–4167.

[9] G. Jayavardhana, B. Rajkumar, M. Slaven, P. Marimuthu, Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, 2013.
[10] S. Hameed, F.I. Khan, B. Hameed, Understanding security requirements and challenges in internet of things (iot): a review, J. Comput. Netw. Commun. (2019) 1–15.
[11] A. Mohammadali, M.S. Haghighi, M.H. Tadayon, A. Mohammadi-Nodooshan, A Novel Identity-Based Key Establishment Method for Advanced Metering Infrastructure in Smart Grid, 2018, https://doi.org/10.1109/TSG.2016.2620939.
[12] P. Gope, A.K. Das, N. Kumar, Y. Cheng, Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks, IEEE Trans. Ind. Inf. 15 (9) (2019) 4957–4968, https://doi.org/10.1109/TII.2019.2895030.
[13] M. Alizadeh, S. Baharun, M. Zamani, T. Khodadadi, M. Darvishi, S. Gholizadeh, H. Ahmadi, Anonymity and untraceability assessment of authentication protocols in PMIPv6, Jurnal Teknologi 72 (5) (2015) 31–34, https://doi.org/10.11113/jt.v72.3936.
[14] K.-K.R. Choo, Z. Yan, W. Meng, Blockchain in industrial IoT applications: security and privacy advances, challenges and opportunities, IEEE Trans. Ind. Inf. 16 (6) (2020) 4119–4121.
[15] S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, Proposed Embedded Security Framework for Internet of Things, IoT, 2011, https://doi.org/10.1109/WIRELESSVITAE.2011.5940923.
[16] W. Stallings, L. Brown, M.D. Bauer, Cryptography and Network Security: Principles and Practice, Pearson Education, New Jursey, 2012.
[17] S. Meng, W. Huang, X. Yin, M.R. Khosravi, Q. Li, S. Wan, L. Qi, Security-aware dynamic scheduling for real-time optimization in cloud-based industrial applications, IEEE Trans. Ind. Inf. 17 (6) (2021) 4219–4228, https://doi.org/10.1109/TII.2020.2995348.
[18] J. Liu, Y. Xiao, C.L. Chen, Internet of Things' Authentication and Access Control, 2012, https://doi.org/10.1504/IJSN.2012.053461.
[19] D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, Internet of things: vision, applications and research challenges, Ad Hoc Netw. 10 (7) (2012) 1497–1516, https://doi.org/10.1016/j.adhoc.2012.02.016.
[20] R.H. Weber, Internet of Things - new security and privacy challenges, Comput. Law Secur. Rep. 26 (2010) 23–30, https://doi.org/10.1016/j.clsr.2009.11.008.
[21] M.C. Domingo, An Overview of the Internet of Underwater Things, 2012, https://doi.org/10.1016/j.jnca.2012.07.012.
[22] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Network. 57 (10) (2013) 2266–2279, https://doi.org/10.1016/j.comnet.2012.12.018.
[23] Z. Yan, P. Zhang, A.V. Vasilakos, A Survey on Trust Management for Internet of Things, 2014, https://doi.org/10.1016/j.jnca.2014.01.014.
[24] M. Alizadeh, M.H. Tadayon, K. Sakurai, H. Anada, A. Jolfaei, A Secure Ticket-based Authentication Mechanism for Proxy Mobile ipv6 Networks in Volunteer Computing 21, 2021, pp. 1–16, https://doi.org/10.1145/3407189, 4.
[25] J. Zhang, X. Du, X. Li, J. Lin, Security key pre-distribution scheme for wireless sensor networks, J. Comput. Appl. 33 (07) (2013) 1851-1853.
[26] M. Alizadeh, K. Sakurai, M. Zamani, S. Baharun, H. Anada, Cryptanalysis of " A secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks, Int. J. Comput. Sci. Bus. Inf. 15 (4) (2015) 40–48.
[27] S. Ch, N. Uddin, M. Sher, A. Ghani, H. Naqvi, A. Irshad, An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography, Multimed. Tool. Appl. 74 (5) (2015) 1711–1723, https://doi.org/10.1007/s11042-014-2283-9.
[28] S.A. Chaudhry, M.S. Farash, H. Naqvi, M. Sher, A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography, Electron. Commer. Res. 16 (1) (2016) 113–139.
[29] K.-K.R. Choo, A proof of revised Yahalom protocol in the Bellare and Rogaway (1993) model, Comput. J. 50 (5) (2007) 591–601.
[30] K.-K.R. Choo, An integrative framework to protocol analysis and repair: Bellare–Rogaway Model+ Planning+ model checker, Informatica 18 (4) (2007) 547–568.
[31] D. He, D. Wang, Robust biometrics-based authentication scheme for multiserver environment, IEEE Syst. J. 9 (3) (2014) 816–823.
[32] M. Burrows, M. Abadi, R. Needham, A logic of authentication, ACM Trans. Comput. Syst. 8 (1990) 18–36, https://doi.org/10.1145/77648.77649.
[33] W.-B. Hsieh, J.-S. Leu, Anonymous authentication protocol based on elliptic curve Diffie–Hellman for wireless access networks, Wireless Commun. Mobile Comput. 14 (10) (2014) 995–1006, https://doi.org/10.1002/wcm.2252.
[34] N. Koblitz, Towards a Quarter-Century of Public Key Cryptography, Springer, 2000.