Formal security analysis of an IoT mutual authentication protocol

Meriam Fariss[1*], *Hassan* El Gafif[1], and *Ahmed* Toumanari[1]

[1]Laboratory of Applied Mathematics and Intelligent Systems Engineering (MAISI), National School of Applied Sciences (ENSA) , 80999 Agadir, Morocco

Abstract. Wireless sensor networks (WSNs) are widely used in day to day activities in order to provide users with multiple services such as smart grids, smart homes, industrial internet of things (IoT), agriculture and health-care. These services are provided by collecting and transmitting the sensing data to the gateway node over an unsafe channel, having constraints of security, energy consumption and connectivity. In 2022, Fariss et al. proposed an ECC-based mutual authentication and key agreement protocol for WSNs. They provided its informal security and showed that it's secure against many security threats. They also formally analyzed the scheme's security using AVISPA Tool. In this article, we analyze the security of Fariss et. Al protocol using GNY logic, an advanced version of BAN logic.

1 Introduction

Wireless Sensor Networks (WSNs) are one of the main parts of Internet of Things (IoT). One of its most important components are sensor nodes. Their main role is to detect and monitor different kinds of data by transmitting it to users through a gateway node that analyzes it. These users should imperatively be legitimate users. The gateway node is not only responsible for data transmission, it also securely stores some private data of sensor nodes and users. One of the biggest security issues in data transmission between the gateway node and the other entities in the network is that the communication channel is public, so anyone can access the network without any control, which exposes it to various attacks.

In fact, if a milicious attacker intercepts the exchanged data between these entities, he/she can recover sensitive information or even disguise as a legitimate party and send incorrect messages to the sensor node or the user. Another challenge related to IoT is the resource constrained devices with limited available power and computational capabilities, which makes the use of lightweight security solutions more suitable for IoT environments.

Many research studies and security protocols were proposed to attain various security objectives. After analyzing some of these protocols, many of them were found to be vulnerable to few attacks even if they were considered to be secure by their designers. That is because one minor mistake may cause the failure of the entire protocol. These minor mistakes are hard to detect informally.

* Corresponding author: meriam.fariss@edu.uiz.ac.ma

As a result, the research community was, and is still trying to create formal security analysis methods to detect as many vulnerabilities as possible in the authentication protocols' designs. One of the wellknown formal security analysis techniques is modal logics that are used to verify that, given a set of assumptions, a set of expected beliefs can be obtained after the execution of the protocol. Burrows–Abadi–Needham (BAN) logic is the milestone when it comes to modal logics. Automated Validation of Internet Security Protocols and Applications (AVISPA) is another formal automated security analysis tool that uses a formal language for specifying security protocols and properties. The protocol can still be vulnerable to an attack that the formal method was not able to detect. Consequently, it is a good practice to analyze an authentication protocol using many formal methods to be more confident about its security.

In this paper, we review an Elliptic Curve Cryptography (ECC) based three-factor mutual authentication and key agreement protocol in WSNs [1]. This protocol's authors provided a security formal analysis using the AVISPA tool alone. To strengthen the proof of the security of this protocol, we provide another formal security analysis using GNY (Gong-Needham-Yahalom) logic, which is an improved version of BAN logic.

The remainder of this paper is organized as follows: In Section II, we present the related work. In Section III, we present an overview of the main preliminaries of the present paper. In Section IV, we provide a formal security analysis of the reviewed protocol using GNY logic. Finally, we give some concluding remarks.

2 Related Work

In the past few years, many authentication schemes have been proposed for WSN environments. In 2007, Tseng et al. [2] proposed a dynamic user authentication scheme [3]. They provided an informal security analysis of their protocol and showed that it can withstand replay attack and forgery attack. Subsequently, Das [4] suggested a hash-based user authentication protocol that uses two factors: passwords and smart cards. He also provided an informal security analysis of his protocol and showed that it can resist many attacks such as replay attack and impersonation attack. However, Nyang and Lee [5] showed that Das's protocol is vulnerable to password guessing attacks performed by insiders and to node compromise attacks. Xue et al. [6] proposed a temporal-credential-based mutual authentication and key agreement scheme. They claimed that it allows mutual authentication among the user, the gateway node (GWN), and the sensor node. It is also secure against many attacks such as masquerade and replay attacks. Thereafter, He et al. [7] suggested another temporal-credential-based mutual authentication and key agreement protocol. They formally analyzed its security using BAN logic and proved that it allows a secure session key and identity sharing between the user and the sensor node. They also proved that their scheme can overcome the security flaws detected in Xue et al.'s protocol, namely user anonymity, offline password guessing attacks, and user and sensor node attacks. Qi and Chen [8] suggested an ECC-based mutual authentication and key agreement scheme that uses biometrics. They claimed that their scheme provides session key agreement and is robust against multiple known attacks. Moreover, using BAN logic, they demonstrated that their scheme provides secure mutual authentication. Nonetheless, in 2019, Sahoo et al. [9] discovered that the scheme is vulnerable to many attacks such as key compromise impersonation attack and offline password guessing attack. Thereafter, they proposed a mutual authentication scheme based on biometrics and ECC. They asserted that their scheme is resistant to replay attacks, stolen smart cards, and offline password guessing. However, in 2022, Ryu et al. [10] demonstrated that this proposed protocol cannot resist insider and privileged insider attacks. Moreover, it cannot provide patient anonymity. To address these security flaws, they proposed an ECC-based three-factor mutual authentication protocol for

telecare medical information systems. Through formal security analysis using BAN logic, AVISPA, and Real-Or-Random (ROR) model, they proved that this protocol can prevent various security attacks. Gope P et al. [11] proposed a lightweight and physically secure anonymous mutual authentication protocol for real-time data access in Industrial Wireless Sensor Networks (IWSNs) using Physical Unclonable Funcions (PUF). They formally analyzed the security of their protocol using the ROR model. Subsequently, Moghadam et al. [12] designed an efficient authentication and key agreement scheme based on Elliptic-Curve Diffie–Hellman (ECDH). The proposed protocol is claimed to support the dynamic node addition and allows the generation of a unique symmetric key and session key for each session. Moreover, the security simulation using Scyther validation tool [13] and the informal security analysis showed that the protocol is secure againt many attacks such as reply attack, Denial of Service (DOS) attack, and known-session-specific temporary information attack. In 2021, Deok et al. [14] proved that Moghadam et al.'s scheme does not achieve perfect forward secrecy. To overcome this security issue, they proposed a secure and lightweight mutual authentication protocol and they proved its security using BAN logic, ROR model, and AVISPA simulation tool.

In 2022, Fariss et al. [1] proposed an ECC-based mutual authentication and key agreement protocol for WSNs. They informally proved that their protocol is secure against many attacks notably, insider attacks, offline password guessing, impersonation attacks, and cloning attacks. The authors used the AVISPA tool to analyze the security of their protocol. However, as we can notice from the previously discussed contributions (e.g., Qi and Chen's scheme [8]), relying on the informal security analysis and only one formal security analysis method does not give us sufficient confidence in the security of the protocol. Consequently, in this paper, we aim to, additionally, analyze this work using the GNY logic, an advanced version of BAN logic.

3 Preliminaries

This section gives an overview of the basic concepts used in this paper including ECC and belief based formal security analysis especially BAN logic and its extended version GNY logic.

3.1 Elliptic Curve Cryptography

To provide better security with a smaller key size, Koblitz [15] and Miller [16] proposed ECC as a type of public-key cryptography. Let $E(F_P)$ denote an elliptic curve over a prime finite field F_P. $E(F_P)$ is defined by (1) where p>3 and the discriminant $\Delta=4a^3+27b^2\neq 0 \pmod p$:

$$y^2=x^3+ax+b \quad ,a,b \in F_p \tag{1}$$

The point O that is equal to (–P)+P is called the point at infinity. All the points of the cyclic additive group G are generated by a generator point P and the order of P is the smallest integer that verifies $n \times P=O$, where × denotes the elliptic curve point multiplication operation. The point multiplication over the elliptic curve can be summarized as follows: given two points P and Q on the elliptic curve and an integer k, Q=kP means that the point Q is equal to P+P+⋯+P (k times). The security provided by ECC can be summarized in the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). The ECDLP states that given two points P and Q=kP on an elliptic curve $E(F_P)$, it is computationally hard to find k. k is called discrete logarithm of Q to the base P.

3.2 GNY logic (Gong-Needham-Yahalon)

BAN logic was invented in 1989. It was the start of the field of formal security analysis. It is a modal logic of knowledge and beliefs and it soon became a milestone in protocol security analysis. This pioneer work is characterized by its simplicity and strong analytic capability. It is used to detect major security threats and to prove the correctness of a protocol. In 1990, Gong et al. [17] extended BAN logic to GNY logic that covers a broad range of protocols. This method aims to prove whether the protocol reaches its goals. It considers belief as a systematic way of understanding how cryptographic protocols work. In comparison with BAN logic, GNY logic requires less universal assumptions such as redundancy in encrypted messages. Moreover, GNY logic allows reasoning about different levels of trust due to the separation between the physical world and the principal beliefs.

4 Formal security analysis using GNY logic

In this section, we provide a formal security analysis of the reviewed protocol using GNY logic. We cite here some of GNY logic notions used in our analysis:

- The notion of possession
- The notion of honesty and competence
- The notion of message extension
- The not-originated-here notion

4.1 Postulates

First, we provide the inference rules used in our analysis and the description of each rule. We note that all the following rules are inherited from the GNY logic paper [17] except the Key-Agreement Rules which we developed based on [18].

- Rationality Rule :

(L1) $\frac{\frac{C_1}{C_2}}{\frac{A\equiv C_1}{A\equiv C_2}}$: if a statement C_1 implies a statement C_2, then if A believes C_1 then she is entitled to believe C_2 too.

- Being-Told Rules :

(T1) $\frac{A\lhd(X,Y)}{A\lhd X}$: if A has been told (X,Y), then she has been told X.

(T2) $\frac{A\lhd\{X\}_K \ , \ A\ni K}{A\lhd X}$: if A has been told the message $\{X\}_K$ which is encrypted with a secret key K she possesses, then A is considered to have been told X.

- Possession Rules :

(P1) $\frac{A\lhd X}{A\ni X}$: if A has been told X, then she is capable of possessing X.

(P2) $\frac{A\ni X}{A\ni H(X)}$: if A possesses X, then she is capable of possessing H(X).

(P3) $\frac{A\ni X \ , \ A\ni Y}{A\ni(X,Y)}$: if A possesses X and Y, then she is capable of possessing the concatenation (X,Y).

(P4) $\frac{A\ni(X,Y)}{A\ni X}$: if A possesses (X,Y), then she is capable of possessing X.

- Freshness Rules :

(F1) $\frac{A\equiv\#(X)}{A\equiv\#(X,Y)}$: if A believes X is fresh, then she is entitled to believe that any formula consisting of X is fresh too.

(F2) $\frac{A\equiv\#(X) \ , \ A\ni X}{A\equiv\#H(X)}$: if A believes X is fresh and possesses X, then she is entitled to believe that H(X) is fresh too.

- Key-Agreement Rules :

(K1) $\frac{A\equiv PK_\delta(B)\ ,\ A\equiv PK_\delta^{-1}(A)}{A\equiv A\overset{K}{\leftrightarrow}B}$ where $K = f(PK_\delta^{-1}(A), PK_\delta(B))$: if A believes in B's key-agreement public key and believes in her own key-agreement private key $PK_\delta^{-1}(A)$, then A is entitled to believe that the key K computed using these two key-agreement keys is a good secret key between A and B.

(K2) $\frac{A\ni PK_\delta(B)\ ,\ A\ni PK_\delta^{-1}(A)}{A\ni K}$ where $K = f(PK_\delta^{-1}(A), PK_\delta(B))$: if A possesses B's key-agreement public key and her own key-agreement private key $PK_\delta^{-1}(A)$, then A is capable of possessing the key K computed using these two key-agreement keys.

(K3) $\frac{A\equiv\#(PK_\delta(B))\ ,\ A\equiv\#(PK_\delta^{-1}(A))}{A\equiv\#K}$ where $K = f(PK_\delta^{-1}(A), PK_\delta(B))$: if A believes that B's key-agreement public key or her own key-agreement private key $PK_\delta^{-1}(A)$ are fresh, then A is entitled to believe that the key K computed using these two key-agreement keys is fresh too.

(K4) $\frac{A\equiv PK_\delta^{-1}(A))}{A\equiv PK_\delta(A))}$: if A believes in her key-agreement private key $PK_\delta^{-1}(A)$, then A is entitled to believe in the corresponding key-agreement public key $PK_\delta(A)$.

(K5) $\frac{A\equiv \#PK_\delta^{-1}(A))}{A\equiv \#PK_\delta(A))}$: if A believes that her key-agreement private key $PK_\delta^{-1}(A)$ is fresh, then A is entitled to believe that the corresponding key-agreement public key $PK_\delta(A)$ is fresh too.

- Message-Interpretation Rules :

(I1) $\frac{A\triangleleft{*}H(X,\langle K\rangle)\ ,\ A\ni(X,K)\ ,\ A\equiv A\overset{K}{\leftrightarrow}B\ ,\ A\equiv\#(X,K)}{A\equiv B|\sim(X,\langle K\rangle)\ \ ,\ \ A\equiv B|\sim H(X,\langle K\rangle)}$: if A has been told a formula H(X,⟨K⟩) which is not-originated-here (A did not generate it before in the actual protocol run), A possesses (X,K), A believes K is a good shared secret between A and B, and A believes (X,K) is fresh, then A is intended to believe that B once conveyed (X,⟨K⟩) and H(X,⟨K⟩).

(I2) $\frac{A\equiv B|\sim X\ ,\ A\equiv\#(X)}{A\equiv B\ni X}$: if A believes that B once conveyed a formula X and A believes X is fresh, then A is entitled to believe that B possesses X.

- Jurisdiction Rules :

(J1) $\frac{A\equiv B\Rightarrow B\equiv *\ ,\ A\equiv B|\sim(X\rightsquigarrow C)\ ,\ A\equiv\#(X)}{A\equiv B\equiv C}$: if A believes that B has jurisdiction over his own beliefs (honest and competent), A believes B once conveyed X⇝C, and A believes X is fresh, then A is entitled to believe that B believes C.

(J2) $\frac{A\equiv B\Rightarrow C\ ,\ A\equiv B\equiv C}{A\equiv C}$: if A believes that B has jurisdiction over a statement C, A believes that B is entitled to believe C, then A is entitled to believe C too.

4.2 Idealized Protocol

- **Message 1**: $\mathrm{U_i} \rightarrow \mathrm{GWN}$: $\left\{\mathrm{ID_i}, \mathrm{SID_j}\right\}_{\mathrm{H}(\mathrm{x_1})}, \mathrm{PK_\delta}(\mathrm{U_i}, \mathrm{E_i}), \mathrm{TS_i},$
$\mathrm{H}\left(\mathrm{ID_i}, \mathrm{SID_j}, \mathrm{TS_i}, \mathrm{PK_\delta}(\mathrm{U_i}, \mathrm{E_i}), \langle \mathrm{x_2}\rangle\right) \rightsquigarrow \mathrm{U_i} \equiv \left(\mathrm{PK_\delta^{-1}}(\mathrm{U_i}, \mathrm{E_i}), \#\mathrm{PK_\delta^{-1}}(\mathrm{U_i}, \mathrm{E_i}), \mathrm{U_i} \ni \mathrm{PK_\delta^{-1}}(\mathrm{U_i}, \mathrm{E_i})\right)$
- **Message 2:** $\mathrm{GWN} \rightarrow \mathrm{S_j}$: $\mathrm{PK_\delta}(\mathrm{U_i}, \mathrm{E_i}), \mathrm{TS_{G1}}, \mathrm{H}(\mathrm{PK_\delta}(\mathrm{U_i}, \mathrm{E_i}), \mathrm{TS_{G1}}, \langle \mathrm{K_{GWN-S}}\rangle) \rightsquigarrow GWN \equiv (PK_\delta(U_i, E_i), \#PK_\delta(U_i, E_i), U_i \equiv (PK_\delta^{-1}(U_i, E_i), \#PK_\delta^{-1}(U_i, E_i)), U_i \ni PK_\delta^{-1}(U_i, E_i))$
- **Message 3:** $\mathrm{S_j} \rightarrow \mathrm{GWN}$: $\mathrm{PK_\delta}\left(\mathrm{S_j}, \mathrm{E_j}\right), \mathrm{TS_j}, \mathrm{H}(\mathrm{PK_\delta}\left(\mathrm{S_j}, \mathrm{E_j}\right), \mathrm{TS_j}, \langle \mathrm{K_{GWN-S}}\rangle) \rightsquigarrow S_j \equiv (PK_\delta^{-1}\left(S_j, E_j\right), \#PK_\delta^{-1}\left(S_j, E_j\right), S_j \ni PK_\delta^{-1}\left(S_j, E_j\right),\ PK_\delta(U_i, E_i), \#PK_\delta(U_i, E_i), S_j \ni PK_\delta(U_i, E_i))$

- **Message 4:** GWN → U_i: $PK_\delta(S_j, E_j), TS_{G2}, H(PK_\delta(S_j, E_j), TS_{G2}, \langle x_2 \rangle) \rightsquigarrow GWN \equiv (PK_\delta(S_j, E_j), \#PK_\delta(S_j, E_j), S_j \equiv PK_\delta^{-1}(S_j, E_j), S_j \equiv \#PK_\delta^{-1}(S_j, E_j), S_j \ni PK_\delta^{-1}(S_j, E_j), S_j \equiv PK_\delta(U_i, E_i), S_j \equiv \#PK_\delta(U_i, E_i), S_j \ni PK_\delta(U_i, E_i))$

GNY proposed the following two checks to test whether a protocol is consistent and valid or not:

- Possession consistency (i.e. a principal should only be able to include in any message he sends, a formula he possesses): obviously, the reviewed protocol is valid according to this check since all the formulae contained in the messages are whether generated or previously received by the sender.

- Belief consistency (i.e. a message extension should include only beliefs held by the sender at the time the message is sent): The message extension in the first communication is valid since all the beliefs included in this message extension are provided as assumptions of U_i (see the assumptions A5, A6, and A7 below)

The message extension appended to the second communication is valid since before sending the message, GWN believes in all the statements included in this message extension (see the beliefs B16, B17, B18, and B19 below)

The message extension appended to the third communication is valid since before sending the message, S_j believes in all the statements included in this message extension (see the assumptions A23, A24, and A25 and the beliefs B23, B29, and B30 below)

The message extension appended to the fourth communication is valid since before sending the message, GWN believes in all the statements included in this message extension (see the beliefs B43, B44, B46, B47, B51, B52, B53, and B54 below)

4.3 Assumptions

(A1) $U_i \equiv PK_\delta(GWN, X_{GWN})$
(A2) $U_i \ni PK_\delta(GWN, X_{GWN})$
(A3) $U_i \equiv PK_\delta^{-1}(U_i, T_i)$
(A4) $U_i \ni PK_\delta^{-1}(U_i, T_i)$
(A5) $U_i \equiv PK_\delta^{-1}(U_i, E_i)$
(A6) $U_i \ni PK_\delta^{-1}(U_i, E_i)$
(A7) $U_i \equiv \#PK_\delta^{-1}(U_i, E_i)$
(A8) $U_i \equiv \#(TS_{G2})$
(A9) $U_i \equiv (GWN \mapsto GWN \equiv *)$
(A10) $U_i \equiv (GWN \mapsto (PK_\delta(S_j, E_j), \#PK_\delta(S_j, E_j), S_j \equiv PK_\delta^{-1}(S_j, E_j), S_j \equiv \#PK_\delta^{-1}(S_j, E_j), S_j \ni PK_\delta^{-1}(S_j, E_j), S_j \equiv PK_\delta(U_i, E_i), S_j \equiv \#PK_\delta(U_i, E_i), S_j \ni PK_\delta(U_i, E_i))$
(A11) $GWN \equiv PK_\delta^{-1}(GWN, X_{GWN})$
(A12) $GWN \ni PK_\delta^{-1}(GWN, X_{GWN})$
(A13) $GWN \equiv PK_\delta(U_i, T_i)$
(A14) $GWN \ni PK_\delta(U_i, T_i)$
(A15) $GWN \equiv S_j \overset{K_{GWN-S}}{\longleftrightarrow} GWN$
(A16) $GWN \ni K_{GWN-S}$
(A17) $GWN \equiv \#(TS_i)$
(A18) $GWN \equiv \#(TS_j)$
(A19) $GWN \equiv (U_i \mapsto U_i \equiv *)$
(A20) $GWN \equiv (U_i \mapsto (PK_\delta^{-1}(U_i, E_i), \#PK_\delta^{-1}(U_i, E_i), U_i \ni PK_\delta^{-1}(U_i, E_i)))$
(A21) $GWN \equiv (S_j \mapsto S_j \equiv *)$
(A22) $GWN \equiv (S_j \mapsto (PK_\delta^{-1}(S_j, E_j), \#PK_\delta^{-1}(S_j, E_j), S_j \ni PK_\delta^{-1}(S_j, E_j), S_j \ni PK_\delta(U_i, E_i))$

(A23) $S_j \equiv PK_\delta^{-1}(S_j, E_j)$
(A24) $S_j \ni PK_\delta^{-1}(S_j, E_j)$
(A25) $S_j \equiv \#PK_\delta^{-1}(S_j, E_j)$
(A26) $S_j \equiv S_j \overset{K_{GWN-S}}{\longleftrightarrow} GWN$
(A27) $S_j \ni K_{GWN-S}$
(A28) $S_j \equiv \#(TS_{G1})$
(A29) $S_j \equiv (GWN \Rightarrow GWN \equiv *)$
(A30) $S_j \equiv (GWN \Rightarrow PK_\delta(U_i, E_i), \#PK_\delta(U_i, E_i), U_i \equiv (PK_\delta^{-1}(U_i, E_i), \#PK_\delta^{-1}(U_i, E_i)), U_i \ni PK_\delta^{-1}(U_i, E_i))$

4.4 Protocol Analysis

In the following analysis, the expression (Ai) + (Bj) + (Pk) ⇒ (Bl) means: given the assumption (Ai) and the belief (Bj), and applying the inference rule (Pk) we get the belief (Bl).

Message 1 ⇒ (B1) $GWN \lhd * \{* ID_i, * SID_j\}_{H(x_1)}, * PK_\delta(U_i, E_i), * TS_i, * H(ID_i, SID_j, TS_i, PK_\delta(U_i, E_i), * \langle x_2 \rangle) \rightsquigarrow U_i \equiv (PK_\delta^{-1}(U_i, E_i), \#PK_\delta^{-1}(U_i, E_i), U_i \ni PK_\delta^{-1}(U_i, E_i))$

(B1) + (T1) + (P1) ⇒ (B2) $GWN \ni PK_\delta(U_i, E_i)$
(A12) + (B2) + (K2) ⇒ (B3) $GWN \ni x_1$
where $x_1 = f(PK_\delta^{-1}(GWN, X_{GWN}), PK_\delta(U_i, E_i))$
(B3) + (P2) ⇒ (B4) $GWN \ni H(x_1)$
(B1) + (T1) + (P1) ⇒ (B5) $GWN \ni \{* ID_i, * SID_j\}_{H(x_1)}$
(B4) + (B5) + (T2) + (P1) ⇒ (B6) $GWN \ni (ID_i, SID_j)$
(A11) + (A13) + (K1) ⇒ (B7) $GWN \equiv U_i \overset{x_2}{\leftrightarrow} GWN$
where $x_2 = f(PK_\delta^{-1}(GWN, X_{GWN}), PK_\delta(U_i, T_i))$
(A12) + (A14) + (K2) ⇒ (B8) $GWN \ni x_2$
where $x_2 = f(PK_\delta^{-1}(GWN, X_{GWN}), PK_\delta(U_i, T_i))$
(B1) + (T1) + (P1) ⇒ (B9) $GWN \ni TS_i$
(B2) + (B6) + (B8) + (B9) + (P3) ⇒ (B10) $GWN \ni (ID_i, SID_j, PK_\delta(U_i, E_i), TS_i, x_2)$
(A17) + (F1) ⇒ (B11) $GWN \equiv \#(ID_i, SID_j, PK_\delta(U_i, E_i), TS_i, x_2)$
(B1) + (T1) ⇒ (B12) $GWN \lhd * H(ID_i, SID_j, TS_i, PK_\delta(U_i, E_i), * \langle x_2 \rangle) \rightsquigarrow U_i \equiv (PK_\delta^{-1}(U_i, E_i), \#PK_\delta^{-1}(U_i, E_i), U_i \ni PK_\delta^{-1}(U_i, E_i))$
(B12) + (B7) + (B10) + (B11) + (I1) ⇒ (B13) $GWN \equiv U_i | \sim H(ID_i, SID_j, TS_i, PK_\delta(U_i, E_i), \langle x_2 \rangle) \rightsquigarrow U_i \equiv (PK_\delta^{-1}(U_i, E_i), \#PK_\delta^{-1}(U_i, E_i), U_i \ni PK_\delta^{-1}(U_i, E_i))$
(B10) + (B11) + (F2) ⇒ (B14) $GWN \equiv \#H(ID_i, SID_j, PK_\delta(U_i, E_i), TS_i, x_2)$
(A19) + (B13) + (B14) + (J1) ⇒ (B15) $GWN \equiv U_i \equiv U_i \equiv (PK_\delta^{-1}(U_i, E_i), \#PK_\delta^{-1}(U_i, E_i), U_i \ni PK_\delta^{-1}(U_i, E_i))$
(A19) + (B15) + (J2) ⇒ (B16) $GWN \equiv U_i \equiv (PK_\delta^{-1}(U_i, E_i), \#PK_\delta^{-1}(U_i, E_i), U_i \ni PK_\delta^{-1}(U_i, E_i))$
(A20) + (B16) + (J2) ⇒ (B17) $GWN \equiv (PK_\delta^{-1}(U_i, E_i), \#PK_\delta^{-1}(U_i, E_i), U_i \ni PK_\delta^{-1}(U_i, E_i))$
(B17) + (K4) ⇒ (B18) $GWN \equiv PK_\delta(U_i, E_i)$
(B17) + (K5) ⇒ (B19) $GWN \equiv \#PK_\delta(U_i, E_i)$

Message 2 ⇒ (B20) $S_j \lhd * PK_\delta(U_i, E_i), * TS_{G1}, * H(* PK_\delta(U_i, E_i), TS_{G1}, * K_{GWN-S}) \rightsquigarrow GWN \equiv (PK_\delta(U_i, E_i), \#PK_\delta(U_i, E_i), U_i \equiv (PK_\delta^{-1}(U_i, E_i), \#PK_\delta^{-1}(U_i, E_i)), U_i \ni PK_\delta^{-1}(U_i, E_i))$

(B20) + (P1) ⇒ (B21) $S_j \ni PK_\delta(U_i, E_i),\ TS_{G1},\ H(PK_\delta(U_i, E_i), TS_{G1}, K_{GWN-S})$

(B20) + (T1) ⇒ (B22) $S_j \lhd * H(* PK_\delta(U_i, E_i), TS_{G1},\ K_{GWN-S}) \rightsquigarrow GWN \equiv (PK_\delta(U_i, E_i), \#PK_\delta(U_i, E_i), U_i \equiv (PK_\delta^{-1}(U_i, E_i), \#PK_\delta^{-1}(U_i, E_i)), U_i \ni PK_\delta^{-1}(U_i, E_i))$

(A27) + (B21) + (P4) + (P3) ⇒ (B23) $S_j \ni (PK_\delta(U_i, E_i),\ TS_{G1}, K_{GWN-S})$

(A28) + (F1) ⇒ (B24) $S_j \equiv \#(PK_\delta(U_i, E_i),\ TS_{G1}, K_{GWN-S})$

(A26) + (B22) + (B23) + (B24) + (I1) ⇒ (B25) $S_j \equiv GWN| \sim H(PK_\delta(U_i, E_i), TS_{G1},\ K_{GWN-S}) \rightsquigarrow GWN \equiv (PK_\delta(U_i, E_i), \#PK_\delta(U_i, E_i), U_i \equiv (PK_\delta^{-1}(U_i, E_i), \#PK_\delta^{-1}(U_i, E_i)), U_i \ni PK_\delta^{-1}(U_i, E_i))$

(B23) + (B24) + (F2) ⇒ (B26) $GWN \equiv \#H(PK_\delta(U_i, E_i), TS_{G1},\ K_{GWN-S})$

(A29) + (B25) + (B26) + (J1) ⇒ (B27) $S_j \equiv GWN \equiv GWN \equiv (PK_\delta(U_i, E_i), \#PK_\delta(U_i, E_i), U_i \equiv (PK_\delta^{-1}(U_i, E_i), \#PK_\delta^{-1}(U_i, E_i)), U_i \ni PK_\delta^{-1}(U_i, E_i))$

(A29) + (B27) + (J2) ⇒ (B28) $S_j \equiv GWN \equiv (PK_\delta(U_i, E_i), \#PK_\delta(U_i, E_i), U_i \equiv (PK_\delta^{-1}(U_i, E_i), \#PK_\delta^{-1}(U_i, E_i)), U_i \ni PK_\delta^{-1}(U_i, E_i))$

(A30) + (B28) + (J2) ⇒ (B29) $S_j \equiv PK_\delta(U_i, E_i)$

(B30) $S_j \equiv \#PK_\delta(U_i, E_i)$

(B31) $S_j \equiv U_i \equiv (PK_\delta^{-1}(U_i, E_i), \#PK_\delta^{-1}(U_i, E_i))$

(B32) $S_j \equiv U_i \ni PK_\delta^{-1}(U_i, E_i))$

(A23) + (B29) + (K1) ⇒ (B33) $S_j \equiv U_i \overset{SK}{\leftrightarrow} S_j$

where $SK = f(PK_\delta^{-1}(S_j, E_j), PK_\delta(U_i, E_i))$

(A24) + (B23) + (P4) + (K2) ⇒ (B34) $S_j \ni SK$

where $SK = f(PK_\delta^{-1}(S_j, E_j), PK_\delta(U_i, E_i))$

(A25) + (B30) + (K3) ⇒ (B35) $S_j \equiv \#SK$

where $SK = f(PK_\delta^{-1}(S_j, E_j), PK_\delta(U_i, E_i))$

Message 3 ⇒ (B36) $GWN \lhd * PK_\delta(S_j, E_j), * TS_j, * H(PK_\delta(S_j, E_j), TS_j, K_{GWN-S}) \rightsquigarrow S_j \equiv (PK_\delta^{-1}(S_j, E_j), \#PK_\delta^{-1}(S_j, E_j), S_j \ni PK_\delta^{-1}(S_j, E_j), PK_\delta(U_i, E_i), \#PK_\delta(U_i, E_i), S_j \ni PK_\delta(U_i, E_i))$

(B36) + (P1) ⇒ (B37) $GWN \ni (PK_\delta(S_j, E_j), TS_j, H(PK_\delta(S_j, E_j), TS_j, K_{GWN-S}))$

(B36) + (T1) ⇒ (B38) $GWN \lhd * H(PK_\delta(S_j, E_j), TS_j, K_{GWN-S}) \rightsquigarrow S_j \equiv (PK_\delta^{-1}(S_j, E_j), \#PK_\delta^{-1}(S_j, E_j), S_j \ni PK_\delta^{-1}(S_j, E_j),\ PK_\delta(U_i, E_i), \#PK_\delta(U_i, E_i), S_j \ni PK_\delta(U_i, E_i))$

(A16) + (B37) + (P4) + (P3) ⇒ (B39) $GWN \ni (PK_\delta(S_j, E_j), TS_j, K_{GWN-S})$

(A18) + (F1) ⇒ (B40) $GWN \equiv \#(PK_\delta(S_j, E_j), TS_j, K_{GWN-S})$

(A15) + (B38) + (B39) + (B40) + (I1) ⇒ (B41) $GWN \equiv S_j| \sim H(PK_\delta(S_j, E_j), TS_j, K_{GWN-S})) \rightsquigarrow S_j \equiv (PK_\delta^{-1}(S_j, E_j), \#PK_\delta^{-1}(S_j, E_j), S_j \ni PK_\delta^{-1}(S_j, E_j), PK_\delta(U_i, E_i), \#PK_\delta(U_i, E_i), S_j \ni PK_\delta(U_i, E_i))$

(A21) + (B41) + (B40) + (J1) ⇒ (B42) $GWN \equiv S_j \equiv S_j \equiv (PK_\delta^{-1}(S_j, E_j), \#PK_\delta^{-1}(S_j, E_j), S_j \ni PK_\delta^{-1}(S_j, E_j),\ PK_\delta(U_i, E_i), \#PK_\delta(U_i, E_i), S_j \ni PK_\delta(U_i, E_i))$

(A21) + (B42) + (J2) ⇒ (B43) $GWN \equiv S_j \equiv PK_\delta^{-1}(S_j, E_j)$

(B44) $GWN \equiv S_j \equiv \#PK_\delta^{-1}(S_j, E_j)$

(B45) $GWN \equiv S_j \equiv S_j \ni PK_\delta^{-1}(S_j, E_j)$

(B46) $GWN \equiv S_j \equiv PK_\delta(U_i, E_i)$

(B47) $GWN \equiv S_j \equiv \#PK_\delta(U_i, E_i))$

(B48) $GWN \equiv S_j \equiv S_j \ni PK_\delta(U_i, E_i))$

(A22) + (B43) + (J2) ⇒ (B49) $GWN \equiv PK_\delta^{-1}(S_j, E_j)$

(A22) + (B44) + (J2) ⇒ (B50) $GWN \equiv \#PK_\delta^{-1}(S_j, E_j)$

(B49) + (K4) ⇒ (B51) $GWN \equiv PK_\delta(S_j, E_j)$

(B50) + (K5) ⇒ (B52) $GWN \equiv \#PK_\delta(S_j, E_j)$

(A22) + (B45) + (J2) ⇒ (B53) $GWN \equiv S_j \ni PK_\delta^{-1}(S_j, E_j)$

(A22) + (B48) + (J2) ⇒ (B54) $GWN \equiv S_j \ni PK_\delta(U_i, E_i)$

Message 4 ⇒ (B55) $U_i \lhd * PK_\delta(S_j, E_j), * TS_{G2}, * H(PK_\delta(S_j, E_j), TS_{G2}, x_2) \rightsquigarrow GWN \equiv (PK_\delta(S_j, E_j), \#PK_\delta(S_j, E_j), S_j \equiv PK_\delta^{-1}(S_j, E_j), S_j \equiv \#PK_\delta^{-1}(S_j, E_j), S_j \ni PK_\delta^{-1}(S_j, E_j), S_j \equiv PK_\delta(U_i, E_i), S_j \equiv \#PK_\delta(U_i, E_i), S_j \ni PK_\delta(U_i, E_i))$

(A1) + (A3) + (K1) ⇒ (B56) $U_i \equiv U_i \overset{x_2}{\leftrightarrow} GWN$

where $x_2 = f(PK_\delta^{-1}(U_i, T_i), PK_\delta(GWN, X_{GWN}))$

(A2) + (A4) + (K2) ⇒ (B57) $U_i \ni x_2$

where $x_2 = f(PK_\delta^{-1}(U_i, T_i), PK_\delta(GWN, X_{GWN}))$

(B55) + (P4) ⇒ (B58) $U_i \ni (PK_\delta(S_j, E_j), TS_{G2})$

(B58) + (B57) + (P3) ⇒ (B59) $U_i \ni (PK_\delta(S_j, E_j), TS_{G2}, x_2)$

(A8) + (F1) ⇒ (B60) $U_i \equiv \#(PK_\delta(S_j, E_j), TS_{G2}, x_2)$

(B55) + (T1) ⇒ (B61) $U_i \lhd * H(PK_\delta(S_j, E_j), TS_{G2}, x_2)$

(B56) + (B59) + (B60) + (B61) + (I1) ⇒ (B62) $U_i \equiv GWN| \sim H(PK_\delta(S_j, E_j), TS_{G2}, x_2)) \rightsquigarrow GWN \equiv (PK_\delta(S_j, E_j), \#PK_\delta(S_j, E_j), S_j \equiv PK_\delta^{-1}(S_j, E_j), S_j \equiv \#PK_\delta^{-1}(S_j, E_j), S_j \ni PK_\delta^{-1}(S_j, E_j), S_j \equiv PK_\delta(U_i, E_i), S_j \equiv \#PK_\delta(U_i, E_i), S_j \ni PK_\delta(U_i, E_i))$

(A9) + (B60) + (B62) + (J1) ⇒ (B63) $U_i \equiv GWN \equiv GWN \equiv (PK_\delta(S_j, E_j), \#PK_\delta(S_j, E_j), S_j \equiv PK_\delta^{-1}(S_j, E_j), S_j \equiv \#PK_\delta^{-1}(S_j, E_j), S_j \ni PK_\delta^{-1}(S_j, E_j), S_j \equiv PK_\delta(U_i, E_i), S_j \equiv \#PK_\delta(U_i, E_i), S_j \ni PK_\delta(U_i, E_i))$

(A9) + (B63) + (J2) ⇒ (B64) $U_i \equiv GWN \equiv (PK_\delta(S_j, E_j), \#PK_\delta(S_j, E_j), S_j \equiv PK_\delta^{-1}(S_j, E_j), S_j \equiv \#PK_\delta^{-1}(S_j, E_j), S_j \ni PK_\delta^{-1}(S_j, E_j), S_j \equiv PK_\delta(U_i, E_i), S_j \equiv \#PK_\delta(U_i, E_i), S_j \ni PK_\delta(U_i, E_i))$

(A10) + (B64) + (J2)⇒ (B65) $U_i \equiv PK_\delta(S_j, E_j)$

(B66) $U_i \equiv \#PK_\delta(S_j, E_j)$

(B67) $U_i \equiv S_j \equiv PK_\delta^{-1}(S_j, E_j)$

(B68) $U_i \equiv S_j \equiv \#PK_\delta^{-1}(S_j, E_j)$

(B69) $U_i \equiv S_j \ni PK_\delta^{-1}(S_j, E_j)$

(B70) $U_i \equiv S_j \equiv PK_\delta(U_i, E_i)$

(B71) $U_i \equiv S_j \equiv \#PK_\delta(U_i, E_i)$

(B72) $U_i \equiv S_j \ni PK_\delta(U_i, E_i)$

(A5) + (B65) + (K1) ⇒ (B73) $U_i \equiv U_i \overset{SK}{\leftrightarrow} S_j$

where $SK = f(PK_\delta^{-1}(U_i, E_i), PK_\delta(S_j, E_j))$

(A6) + (B58) + (P4) + (K2) ⇒ (B74) $U_i \ni SK$

where $SK = f(PK_\delta^{-1}(U_i, E_i), PK_\delta(S_j, E_j))$

(A7) + (B66) + (K3) ⇒ (B75) $U_i \equiv \#SK$

where $SK = f(PK_\delta^{-1}(U_i, E_i), PK_\delta(S_j, E_j))$

(B67) + (B70) + (K1) + (L1) ⇒(B76) $U_i \equiv S_j \equiv U_i \overset{SK}{\leftrightarrow} S_j$

where $SK = f(PK_\delta^{-1}(S_j, E_j), PK_\delta(U_i, E_i))$
(B69) + (B72) + (K2) + (L1) ⇒ (B77) $U_i \equiv S_j \ni SK$
where $SK = f(PK_\delta^{-1}(S_j, E_j), PK_\delta(U_i, E_i))$
(B68) + (B71) + (K3) + (L1) ⇒ (B78) $U_i \equiv S_j \equiv \#SK$
where $SK = f(PK_\delta^{-1}(S_j, E_j), PK_\delta(U_i, E_i))$

4.5 Achieved goals

We conclude that given the aforementioned assumptions and following the reviewed protocol, principals U_i and S_j achieve the following goals:

Ui's goals :

$U_i \equiv U_i \overset{SK}{\leftrightarrow} S_j$, $U_i \ni SK$, $U_i \equiv \#SK$

$U_i \equiv S_j \equiv U_i \overset{SK}{\leftrightarrow} S_j$, $U_i \equiv S_j \ni SK$, $U_i \equiv S_j \equiv \#SK$

Sj's goals :

$S_j \equiv U_i \overset{SK}{\leftrightarrow} S_j$, $S_j \ni SK$,$S_j \equiv \#SK$

$S_j \equiv U_i \equiv PK_\delta^{-1}(U_i, E_i)$, $S_j \equiv U_i \equiv \#PK_\delta^{-1}(U_i, E_i)$, $S_j \equiv U_i \ni PK_\delta^{-1}(U_i, E_i))$

5 Conclusion

In this paper, we extended the formal security analysis of [1] using GNY Logic. Our security analysis proves that, as claimed, the reviewed protocol successfully achieves mutual authentication and key-agreement between the user and the sensor. Additionally, the provided formal analysis enabled us to explicitly define all the assumptions needed to be guaranteed in order to achieve mutual authentication and key-agreement after executing the protocol. For instance, one obvious assumption is that both the sensor and the user need to fully trust the GWN. Generally, this is considered as a weak assumption. However, this also makes the GWN a single point of failure. Henceforth, in the future, we aim to get rid of this assumption and develop a decentralized version of the reviewed protocol.

References

1. M. Fariss, H. El Gafif, A. Toumanari, *A Lightweight ECC-Based Three-Factor Mutual Authentication and Key Agreement Protocol for WSNs in IoT*, IJACSA, **13** (2022)
2. H.-R. Tseng, R.-H. Jan, W. Yang, *An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks*, in Proceedings of the Global Communications Conference, GLOBECOM, 26-30 November 2007, Washington, DC, USA (2007)
3. P. S. Teh, N. Zhang, A. B. J. Teoh, K. Chen, *A survey on touch dynamics authentication in mobile devices*, Comput. Secur. **59** 210–235 (2016)
4. M. L. Das, *Two-factor user authentication in wireless sensor networks*, *IEEE Trans Commun* **8** 1086–1090 (2009)
5. D. Nyang, M.-K. Lee, *Improvement of Das's Two-Factor Authentication Protocol in Wireless Sensor Networks*, *IACR Cryptology ePrint Archive*, **2009** 631 (2009)
6. K. Xue, C. Ma, P. Hong, R. Ding, *A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks*, J. Netw. Comput. Appl., **36** 316–323 (2013)
7. D. He, N. Kumar, N. Chilamkurti, *A secure temporal-credential-based mutual*

authentication and key agreement scheme with pseudo identity for wireless sensor networks, Inf. Sci., **321** 263–277 (2015)
8. M. Qi, J. Chen, *New robust biometrics-based mutual authentication scheme with key agreement using elliptic curve cryptography*, Multimed Tools Appl **77**, 23335–23351 (2018)
9. S. S. Sahoo, S. Mohanty, B. Majhi, *Improved Biometric-Based Mutual Authentication and Key Agreement Scheme Using ECC*, Wireless Pers Commun **111**, 991–1017 (2020)
10. J. Ryu, J. Oh, D. Kwon, S. Son, J. Lee, Y. Park, Y. Park, *Secure ECC-Based Three-Factor Mutual Authentication Protocol for Telecare Medical Information System*, IEEE Access **10**, 11511-11526 (2022)
11. 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 Industr Inform **15** 4957–4968 (2019)
12. M. F. Moghadam, M. Nikooghadam, M. A. B. Al Jabban, M. Alishahi, L. Mortazavi, A. Mohajerzadeh, *An Efficient Authentication and Key Agreement Scheme Based on ECDH for Wireless Sensor Network*, IEEE Access **8** 73182–73192 (2020)
13. C. J. F. Cremers, *Scyther: semantics and verification of security protocols*, Eindhoven University of Technology (2006)
14. D. Kwon, S. Yu, J. Lee, S. Son, Y. Park, *Wsn-slap: Secure and lightweight mutual authentication protocol for wireless sensor networks*, Sensors **21** (2021)
15. B. N. Koblitz, *Elliptic Curve Cryptosystems*, Math. Comput. **48** 203–209 (1987)
16. V. S. Miller, *Use of Elliptic Curves in Cryptography*, LNCS **218** 417–426 (1986)
17. L. Gong, R. Needham, R. Yahalom, *Reasoning about Belief in Cryptographic Protocols*, in Proceedings 1990 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, USA, (1990)
18. P. C. van Oorschot, *Extending Cryptographic Logics of Belief to Key Agreement Protocols*, Oorschot, Paul C. van. "Extending cryptographic logics of belief to key agreement protocols." Conference on Computer and Communications Security (1993)