Lightweight, Anonymous and Mutual Authentication in IoT Infrastructure

Shadi Janbabaei
Department of Computer Engineering
Shahed University, Tehran, Iran
sh.janbabaei@shahed.ac.ir

Hossein Gharaee
Iran Telecom. Research Center
Tehran, Iran
gharaee@itrc.ac.ir

Naser Mohammadzadeh
Department of Computer Engineering
Shahed University, Tehran, Iran
mohammadzadeh@shahed.ac.ir

Abstract—Recent development in information technology and internet makes the internet of things (IoT) more popular than before. Since all of entities can be interact with each other, so some security elements such as authentication should be considered. Sensor-to-Sensor connection is one of the important communications in IoT environment. Therefore in this paper, lightweight authentication protocol between sensors in stationary and mobile mode is proposed to be suitable for constraint entities. This protocol can ensure some security and privacy features such as anonymity, untraceability and so on. At the end, security requirements and computational costs between different schemes are compared.

Keywords—Internet of Things; authentication; anonymity; lightweight; untraceablity

I. INTRODUCTION

For the first time, the phrase "Internet of Things (IoT)" was used by Kevin Ashton in 1999. He described IoT as the world in which things have a digital identity and allow computers to organize and manage them [1]. This new paradigm includes wireless sensor networks (WSNs), RFID, machine-to-machine interfaces, cloud services, etc. [2].

IoT is uncontrolled and heterogeneous environment that requires scalability, which is also associated with constrained resources. With consideration of these properties, the security requirements of IoT are classified into five categories: network security, identity management, privacy, trust and resilience. Authentication is an important concept of identity management which is included devices communication and key exchange to prevent data theft. According to the constrained resources in IoT, the authentication protocols should be light weight [3].

On the other hand, anonymity is one of the most essential security requirements in privacy preserving [4]. In fact, intruder should not be able to track users or specify user's identity. So the possibility of several attacks like forgery attack, replay attack and redirection attack are reduced [5, 6].

Consequently, it is desirable to define anonymous, light weight and mutual authentication scheme for IoT environment. According to [7], this protocol is designed but it doesn't support the sensor-to-sensor connections. Also, it is better to establish a session key at the end of the protocol. In [8], the connection between sensors is established, due to utilization of elliptic curve cryptography (ECC), it is not suitable for constrained sensors. Decentralized authentication mechanism for vehicular ad hoc networks (VANETs) are proposed in [9] but it is not as lightweight as [7] and it is specialized for ad hoc networks. So, mutual authentication between sensors in IoT environment is an important issue which is discussed in this paper.

Improvement of authentication and key agreement protocol in IoT environment, protocol analysis, comparing security requirements and computational cost between proposed scheme and other schemes, are main contributions of this paper.

The reminder sections organized as follows. Section 2 provides a brief overview about related work. In section 3, it is presented the proposed lightweight authentication and key agreement scheme. Thereafter, security analysis of proposed scheme is given in section 4. Performance analysis is discussed in section 5. Finally, a conclusion is given in last section.

II. RELATED WORK

In the architecture of IoT, different connections are assumed between entities. In [8, 10, 11] the connection between two sensor nodes (SNs) is investigated so that they are authenticated to each other at first, and a session key is exchanged between them. The connection between end user and sensor is investigated in [7], and it is assumed that the sensor is displaced between different clusters. As a result, an authentication protocol is designed between the Cluster Head (CH) and the mobile sensor. After the authentication, it is better to establish a session key between them and use it to send data or services [5, 8-13]. In [14], two-way authentication scheme for IoT based on DTLS protocol have been explained. Because of using X.509 certificates and RSA public keys with DTLS handshake, this scheme is heavy for constrained SNs. In the proposed scheme, the connection between two sensors is measured in both stationary and mobile modes. This protocol is provided for the authentication between sensors and, ultimately, a session key is exchanged between them.

In many articles anonymity has also been included in the authentication protocol to make user tracking impossible. In general, anonymity is divided into two categories: weak and strong. The weak anonymity is resulted by concealing the entity through coding or encryption methods, but in this case,

978-1-5090-3435-2/16/$31.00 ©2016 IEEE

the entity is easy to be traced due to same output. In the strong anonymity mode, the attacker cannot identify the entity through eavesdropping channels [4]. In the absence of strong anonymity, the attacker can track the user's location. Strong anonymity is used in most articles, in which the sensor uses a one-time-alias. In case of having a repetitive connection with a constant entity, the identity of the user is not recognized. With using anonymity, a lot of attacks including forgery attack, replay attack, redirection attack and etc. become impossible [4-7, 9, 12, 13, 15].

The ECC has been used instead of RSA encryption to have the provided protocols to be more appropriate for nodes with constrained resources [8, 11]. However, these protocols have high computational overheads. In articles [6, 10] the cryptographic functions are used for authentication to somewhat reduce the computational overhead. On the other hand, the Hash and Exclusive OR (XOR) Functions have been used rather than the cryptographic functions to make protocols lighter than ever before [4, 7, 12, 15]. In [7], the mutual authentication protocol is proposed which ensures anonymity and untraceability. In this protocol, authentication is between mobile SN and CH and it is not support the authentication between two sensors. Also, there is not any session key agreement at the end of the protocol. In this paper we investigate the authentication of two sensors so that it is considered anonymous, untraceable and lightweight features.

III. PROPOSED SCHEME

A. Assumed Architecture

In this part, we explain internet of things architecture for modeling proposed authentication protocol. This architecture includes four necessary components: an authenticated cloud server (ACS), network entities such as CH and home IoT server (HIoTS) and edge devices like SNs [7].

According to Fig. 1, components can have connection in hierarchical and horizontal modes. For example, connection between end user and SN is hierarchical whereas connection between two sensors is horizontal. In [7] architecture and hierarchical connection are investigated in sensor movement. Therefore in proposed scheme, we study on connection between two sensors to complete mentioned protocol. Also, the proposed protocol is designed to authenticate in both stationary and mobile modes.

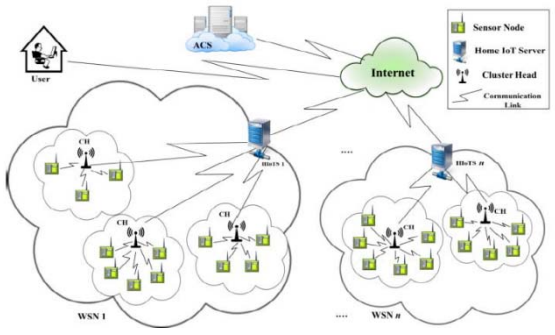

Fig. 2. Distributed IoT system architecture [7]

TABLE I. NOTATIONS

Symbol	Definitions
ID_h	Identity of the HIoTS
ID_{sn}	Identity of SN
AID_{sn}	One-time-alias identity of the SN
N_s,N_p,R_m	Random number
Tr_{seq}	Track sequence number
Sk_i	required keys for generating SK
SK	Session key generated between two sensors
h (.)	One-way hash function
$\oplus$	Exclusive-OR function
$\|\|$	Concatenation function

In this section, an authentication scheme between sensors is proposed. It consists of two phases. First phase that is called registration phase, HIoTS sends security credential to SNs through a secure channel. Sensors are authenticated in second phase. They can be located in same HIoTS or can be stable in their location. Also, in this scheme sensors can move from one cluster to another or their location can be stationary.

1) Registration Phase:

The SN sends its identity to HIoTS through secure channel. Then HIoTS generates a random number and computes $K_{sh} = h (ID_{Sni} \| n_h) \oplus H_{id}$. HIoTS also generates a track sequence number (Tr_{seq}) that is generated randomly. Then it sends Tr_{seq} to the SN and keep a copy in its database [7].

2) Authentication Phase

a) In same HIoTS

In [7], author focused on connection between CH and SN that they authenticate each other but we want to design an authentication protocol between two sensors in same HIoTS. This phase of the scheme consists of the following steps:

Step1: SN_1 computes:

$N_x = K_{sh1} \oplus N_s$

$AID_{sn1} = h (ID_{sn1} \| K_{sh1} \| N_s \| Tr_{seq1})$.

Then, it sends a request message M_1 to SN_2.

$M_1 = \{AID_{sn1}, N_x, Tr_{seq1}, ID_{h1}\}$

Step2: After receiving the request, SN_2 computes:

$N_z = K_{sh2} \oplus N_p$

$AID_{sn2} = h (ID_{sn2} \| K_{sh2} \| N_p \| Tr_{seq2})$

Finally the sensor sends M_2 to its CH.

$M_2 = \{AID_{sn2}, N_z, M_1, Tr_{seq2}, ID_{h2}\}$

Step3: CH sends M_2 to current HIoTS.

Step4: Current HIoTS Checks both ID_{h1} and ID_{h2}.

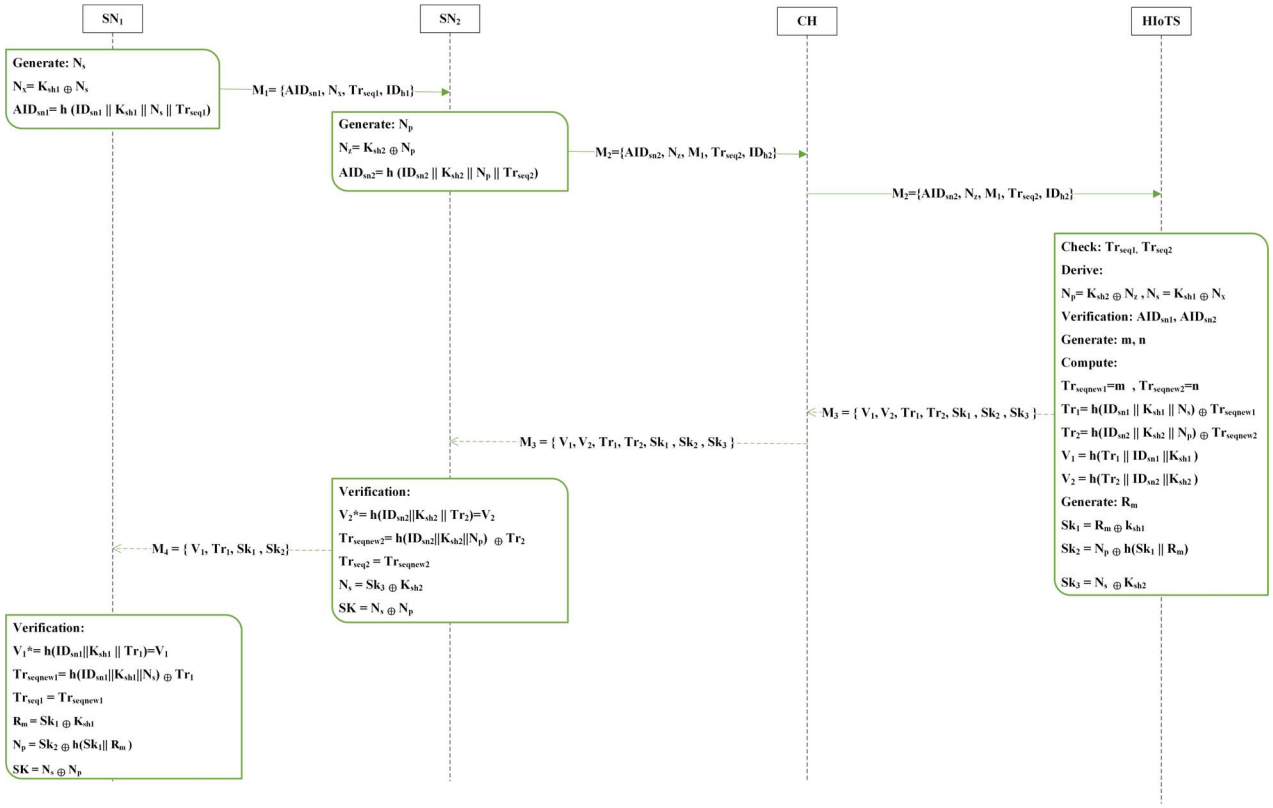

Fig. 2. Proposed protocol for authentication two sensors in a same HIoTS

If they are the same, it compares Tr_{seq1} and Tr_{seq2} with their real values. Also it derives:

$N_p = K_{sh2} \oplus N_z$ and $N_s = K_{sh1} \oplus N_x$.

Then HIoTS Verifies AID_{sn1}, AID_{sn2} and Generates: m, n.

It also computes:

$Tr_{seqnew1}=m$

$Tr_{seqnew2}=n$

$Tr_1 = h (ID_{sn1} \| K_{sh1} \| N_s) \oplus Tr_{seqnew1}$

$Tr_2 = h (ID_{sn2} \| K_{sh2} \| N_p) \oplus Tr_{seqnew2}$

$V_1 = h (Tr_1 \| ID_{sn1} \| K_{sh1})$

$V_2 = h (Tr_2 \| ID_{sn2} \| K_{sh2})$

And it generates: R_m

$Sk_1 = R_m \oplus k_{sh1}$

$Sk_2 = N_p \oplus h (Sk_1 \| R_m)$

$Sk_3 = N_s \oplus K_{sh2}$

Finally, HIoTS issues M_3 to CH.

$M_3 = \{V_1, V_2, Tr_{seq1}, Tr_{seq2}, Sk_1, Sk_2, Sk_3\}$

Step 5: Without any changes, CH sends M_3 to SN_2.

Step 6: SN_2 verifies V_2 and computes:

$Tr_{seqnew2} = h (ID_{sn2} \| K_{sh2} \| N_p) \oplus Tr_2$

$Tr_{seq2} = Tr_{seqnew2}$

$N_s = Sk_3 \oplus K_{sh2}$

$SK = N_s \oplus N_p$

SN_2 sends a response message M4 to SN_1.

$M4 = \{V_1, Tr_1, Sk_1, Sk_2\}$

Step 7: SN_1 verifies V_1 and computes:

$Tr_{seqnew1} = h (ID_{sn1} \| K_{sh1} \| N_s) \oplus Tr_1$

$Tr_{seq1} = Tr_{seqnew1}$

$R_m = Sk_1 \oplus K_{sh1}$

$N_p = Sk_2 \oplus h (Sk_1 \| R_m)$

$SK = N_s \oplus N_p$

All of interactions are shown in Fig. 2.

b) In Different HIoTS

This part is focused on connection between SNs in different HIoT servers. In order to authenticate the SNs, similar protocol of previous section can be used with minor changes. In that case, some functions of current HIoTS should be done by original HIoTS which is belonged to SN_1. Also, it's assumed that interaction between HIoT servers is done in a secure channel. This interaction is shown in Fig. 3.

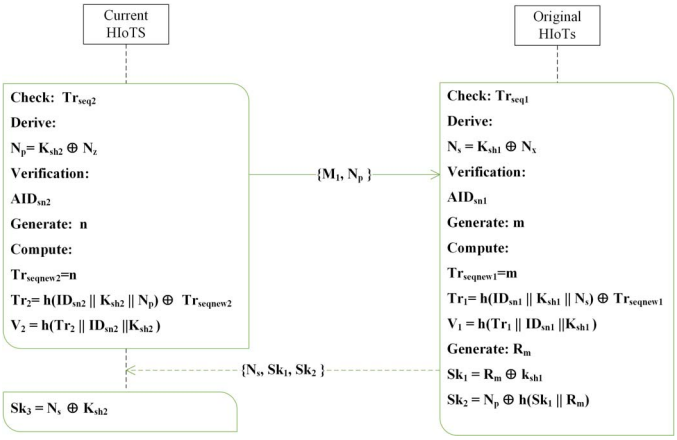

Fig. 3. Connection between different HIoT servers

IV. Security analysis

In this section, an analysis of proposed protocol is presented and important security properties are explained.

- Mutual authentication: In proposed protocol, AID_1 and AID_2 are verified by HIoTS to authenticate SNs. Also, SN_1 and SN_2 verify V_1 and V_2 respectively to authenticate HIoTS. So all of identities are authenticated successfully.
- Anonymous authentication: Using one-time-alias identity makes protocol to be anonymous because adversary cannot discover the real identity of the SNs.
- Untraceability: AID is made of a random number and this number is changed in each connection. In the other word, a dynamic process is used in proposed protocol. So adversary cannot trace sensor's location too.
- Session key agreement: after sensors authentication, they should be able to communicate with each other. Due to unsafe channel, it better to establish a session key at the end of the protocol.

V. Performance analysis and comparison

The purpose of proposed protocol is to solve several issues in IoT environment. In this section, proposed protocol is compared with other schemes. As it is shown in table II, proposed scheme can satisfy important requirements in IoT. In contrast, other protocols cannot satisfy all the features.

In [7], most of the features are supported but it only explained the authentication scheme between SN and CH in a movement state. In Proposed scheme, authentication is performed between two SNs in both movement and stable states. These sensors can be located in same or different HIoT servers. Also, session key agreement is one of the important features at the later steps of protocol.

In addition, all factors are supported in [9], but proposed protocol has less functional cost. Table III determines functional cost of papers.

TABLE II. Performance analysis based on features

	P_1	P_2	P_3	P_4
[14]	×	×	×	×
[8]	✓	×	×	✓
[7]	✓	✓	✓	×
[9]	✓	✓	✓	✓
Proposed	✓	✓	✓	✓

P: Property; P_1: Mutual authentication; P_2: anonymity; P_3: Untraceablity; P_4: Session key agreement

TABLE III. Computational overheads

	Hash	XOR	||
[7]	12	6	28
[9]	19	12	10
Proposed	12	16	30

VI. Conclusion

In this paper, at first a distributed architecture of IoT is explained. Then mutual authentication protocol between two sensors in IoT environment is designed and analyzed. Also, the proposed protocol is anonymous and untraceable. It comprises of three phases: registration phase, authentication phase in same HIoTS and authentication phase in different HIoT servers. In comparison with other schemes, proposed scheme is not more lightweight than other protocols but it has some extra features. For example, it includes key agreement and considers sensor authentication in both stationary and mobile modes. Also, there is no location constraint for sensors. A proposed direction for the future work would be to add trust to the proposed protocol.

VII. References

[1] K. Ashton, "That 'internet of things' thing," *RFiD Journal,* vol. 22, pp. 97-114, 2009.

[2] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks,* vol. 57, pp. 2266-2279, 2013.

[3] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, "On the Security and Privacy of Internet of Things Architectures and Systems," in *International Workshop on Secure Interner of Things(SIOT)* 2015.

[4] P. Gope and T. Hwang, "A Realistic Lightweight Authentication Protocol Preserving Strong Anonymity for Securing RFID System," *Computers & Security,* vol. 55, pp. 271–280, 2015.

[5] P. Gope and T. Hwang, "Enhanced Secure Mutual Authentication and Key Agreement Scheme Preserving User Anonymity in Global Mobile Networks," *Wireless Personal Communications,* vol. 82, pp. 2231-2245, 2015.

[6] T. Hwang and P. Gope, "Provably secure mutual authentication and key agreement scheme with user anonymity," in *Information, Communications and Signal Processing (ICICS) 2013 9th International Conference on*, 2013, pp. 1-5.

[7] P. Gope and T. Hwang, "Untraceable sensor movement in distributed IoT infrastructure," *Sensors Journal, IEEE,* vol. 15, pp. 5340-5348, 2015.

[8] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications," *International Journal of Distributed Sensor Networks,* vol. 2014, 2014.

[9] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," *Systems Journal, IEEE,* vol. 8, pp. 749-758, 2014.

[10] P. N. Mahalle, N. R. Prasad, and R. Prasad, "Threshold Cryptography-based Group Authentication (TCGA) scheme for the Internet of Things (IoT)," in *Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2014 4th International Conference on*, 2014, pp. 1-5.

[11] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in *Wireless Communications and Networking Conference (WCNC), 2014 IEEE*, 2014, pp. 2728-2733.

[12] P. Gope and T. Hwang, "Lightweight and Energy-Efficient Mutual Authentication and Key Agreement Scheme With User Anonymity for Secure Communication in Global Mobility Networks," *Systems Journal, IEEE,* vol. PP, pp. 1 - 10, 2015.

[13] F. Wen, W. Susilo, and G. Yang, "A secure and effective anonymous user authentication scheme for roaming service in global mobility networks," *Wireless personal communications,* vol. 73, pp. 993-1004, 2013.

[14] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, "A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication," in *Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference on*, 2012, pp. 956-963.

[15] P. Gope and T. Hwang, "An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks," *Journal of Network and Computer Applications,* vol. 62, pp. 1-8, 2016.