International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:13, No:2, 2019

Mutual Authentication for Sensor-to-Sensor Communications in IoT Infrastructure

Shadi Janbabaei, Hossein Gharaee Garakani, Naser Mohammadzadeh

***Abstract*—**Internet of things is a new concept that its emergence has caused ubiquity of sensors in human life, so that at any time, all data are collected, processed and transmitted by these sensors. In order to establish a secure connection, the first challenge is authentication between sensors. However, this challenge also requires some features so that the authentication is done properly. Anonymity, untraceability, and being lightweight are among the issues that need to be considered. In this paper, we have evaluated the authentication protocols and have analyzed the security vulnerabilities found in them. Then an improved light weight authentication protocol for sensor-to-sensor communications is presented which uses the hash function and logical operators. The analysis of protocol shows that security requirements have been met and the protocol is resistant against various attacks. In the end, by decreasing the number of computational cost functions, it is argued that the protocol is lighter than before.

***Keywords*—**Anonymity, authentication, Internet of Things, lightweight, untraceablity.

I. Introduction

WITH the advancements in Internet technologies, a new trend in the era of ubiquity is being realized. Huge increase in users of Internet and modifications on the internetworking technologies enable networking of everyday objects.

The Internet of Things is described as a global network of interconnected objects that are addressable and operates based on standard communication protocols. Kevin Ashton introduced the IoT for the first time in 1999. He defined the IoT as the world in which objects have a digital identity and allow computers to organize and manage them [1], [2]. Different technologies such as Radio-frequency identification (RFID), Near Field Communications (NFC), machine to machine (M2M) and vehicle to vehicle (V2V) communications have been used to implement the idea of IoT [3].

Uncontrolled, heterogeneous and scalable environment with constrained resources are IoT properties. According to the constrained resources, the authentication protocols should be light weight so that entities can use them. On the other hand, 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. Also, one of the main parameters in privacy is anonymity [4]. In fact, intruder should not be able to track user's activity or identify user's identity. So the possibility of several attacks like forgery attack, replay attack and redirection attack are reduced [5], [6]. In addition, mutual authentication and key agreement are important issues in the investigation of authentication protocols [7]. Consequently, it seems necessary to propose anonymous, light weight and mutual authentication scheme for sensor-to-sensor communications in IoT environment.

Improved mutual authentication and key agreement protocol in IoT environment, protocol analysis, comparing security requirements, attacks resistance and computational costs between proposed scheme and other schemes, are the main contributions of this paper.

The reminder sections of this paper are organized as follows. Section II provides a brief overview about related works. In Section III, the mutual authentication and key agreement scheme for sensor-to-sensor communications is presented. Thereafter, security analysis of the scheme is given in Section IV. Computational costs and resistance to attacks are discussed in Section V. Finally, a conclusion is given in last section.

II. Related Works

In the IoT architecture, different communications are assumed between entities. In [8]-[10] the communication 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 communications between end user and SN is discussed in [11], and it is assumed that the sensor is displaced between different clusters.

Mutual authentication with a collection of features related to IoT such as anonymity, being lightweight and untraceablity is one of the most important challenges of the day. Various solutions were used to solve this challenge. In a series of protocols, encryption and decryption functions were used that have high computational overhead. In order to reduce this overhead, Elliptic Curve Cryptography (ECC) is used. In [12], end to end architecture for mutual authentication based on Datagram Transport Layer Security (DTLS) was suggested. Eight massages for DTLS handshaking caused a considerable network traffic. On the other hand, due to the use of X.509 certificates and RSA public keys with DTLS handshakes, this protocol is not suitable for constrained sensors. Another

Naser Mohammadzadeh and Shadi Janbabaei are with Department of Computer Engineering, Shahed University, Tehran, Iran (corresponding author, phone: +982151212098; fax: +982151212021; e-mail: mohammadzadeh@shahed.ac.ir).

Hossein Gharaee Garakani is with Department of Network Security and Information Technology Research Center – ITRC, Tehran, Iran (e-mail: gharaee@itrc.ac.ir).

security scheme based on Elliptic Curve Qu-Vanstone (ECQV) and DTLS was presented for IoT in [13]. In this scheme Elliptic curve Diffie–Hellman (ECDH) key agreement algorithm is used and implicit ECQV certificates were applied instead of X.509 certificates.

Recently, lighter functions like the hash function and operators such as Exclusive OR (XOR) and concatenation have been used so that lightweight is provided as an important factor in IoT. In [9] a mutual authentication protocol between two sensors is designed. In this protocol, the anonymity and untraceablity were not included. On the other hand, the session key between two sensors is constant, thus in the case of revealing this key, there will be no chance for further communication. Also, in order to create communication among sensors in different clusters, DTLS communication should be created among Cluster Heads (CHs) that increase computational overheads. In [14], a mutual authentication scheme for Vehicular Ad Hoc Network (VANET) is provided that all the operations of it are committed by Pre-Shared Key (PSK). As a result, if we have a reliable but curious entity, it can easily access all keys and information. So this scheme is not suitable for entities in the context of IoT. Hash based tag authentication protocol is explained in [15]. It does not support anonymity and untraceablity. In addition, [16] claims that mentioned protocol is vulnerable to a novel forgery attack. Another mutual authentication protocol was introduced in [11] that supports anonymity and untraceablity. In this scheme, it is a difficult task that someone recognizes the One-time-alias identity (AID) belongs to which ID. Also, it is good to create a session key at the end of the authentication. Furthermore, contrary to the committed claim, this protocol is vulnerable against replay attack in the returned path. So in this paper, we design a mutual authentication protocol between two sensors so that it considers important features of IoT and defeats different type of attacks.

III. Proposed Scheme

A. Assumed Architecture

In this part, we explain network architecture for modeling proposed authentication protocol [9]. According to Fig. 1, components can have connection in vertical and horizontal modes. For example, connection between end user and SN is hierarchical whereas connection between two sensors is horizontal. However, because of the space limitation, we will emphasize on the authentication of sensors in same CHs, which is an important issue in IoT infrastructure.

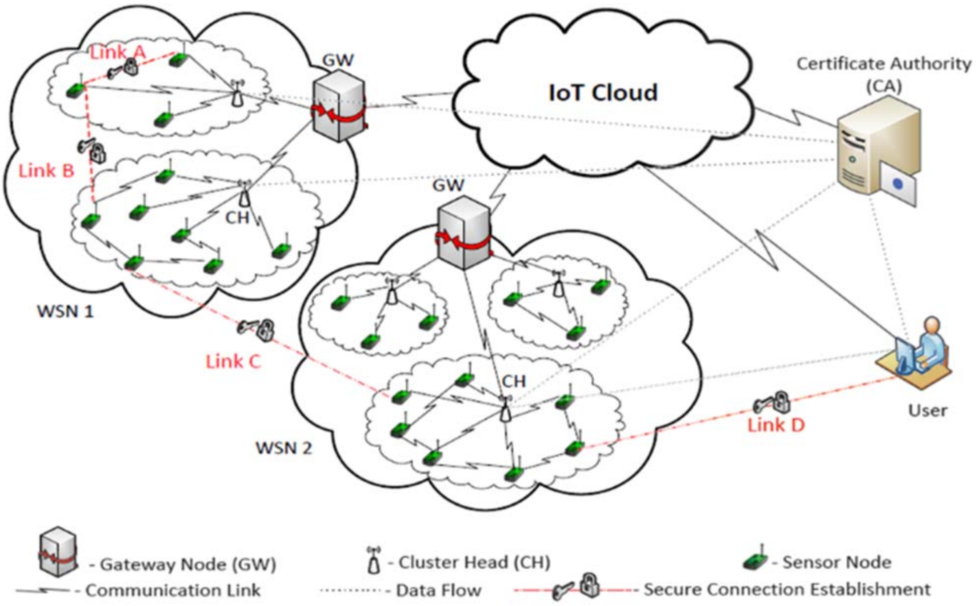

Fig. 1 Network architecture [9]

Proposed scheme consists of two phases. In registration phase, CH sends security credential to SNs through a secure channel and sensors are authenticated to each other in second phase. Both phases are represented in following parts.

1) Registration Phase

The SN sends its identity to CH through secure channel. CH generates random numbers K_i and Tr_i and computes $AID_{sn} = H(ID_{Sn} \| Tr_i)$. Then it sends $\{AID_{sn}, ID_{ch}, Tr_i, K_i, H(.)\}$ to the SN and keep a copy in its database (Fig. 2).

2) Authentication Phase

We design an authentication protocol between two sensors in the same CH. This phase of our scheme consists of the following steps:

Step1. SN1 computes:

$A = N1 \oplus K1$

$V1 = H(AID1 \| AID2 \| N1 \| Tr1)$ or

$AV1 = H(AID1 \| AID2 \| N1 \| ID1)$

TABLE I
NOTATIONS

Symbol	Definition
ID_i	Identity of SNi
AID_i	One-time-alias identity of the SNi
N_i	Random number
Tr_i	Track sequence number
K_i	Agreed key between SNi and CH
Sk_i	Required keys for generating SK
SK	Session key generated between two sensors
V1-V4	Statements to evaluate the received message
AV_i	Alternative Vi
H(.)	One-way hash function
⊕	Exclusive-OR function
||	Concatenation function

Note: i as subscript can be related to SN1 if it's value is "1" and also it can be related to SN2 if it's value is "2".

Then, it sends a request message M1 to CH.

Step2. After receiving the request, CH checks Tr_1, gets N_1 value and verifies V_1. Finally, it sends M_2 to related SN_2 and asks authentication parameters.

Step3. SN_2 has similar computations to SN_1 (step1) and then sends M_3 to CH.

Step4. CH has a similar response to M_3. Then it updates the AID values and computes SK for communicating SNs with each other. At the end, CH computes following parameters and sends M_4 and M_5 to SN_1 and SN_2 respectively.

$$SK_1 = H(Tr_1 \| SK) \oplus H(K_1 \| AID_2)$$
$$SK_2 = H(Tr_2 \| SK) \oplus H(K_2 \| AID_1)$$
$$V_3 = H(AID_1 \| SK_2 \| N_2 \| Tr_2)$$
$$V_4 = H(AID_2 \| SK_1 \| N_1 \| Tr_1)$$

Step5. SN_2 gets SK and Tr_2. According to Tr_2 value, it verifies V_3 and computes AID_{new2}. Finally, SN_2 updates the AID_2 to use in other connections.

Step6. By receiving M_4, SN_1 has a similar reaction. It gets SK and Tr_1, verifies V_4 and computes AID_{new1}. Finally, SN_1 updates the AID_1 to use in other connections. All of interactions are shown in Fig. 3.

IV. SECURITY ANALYSIS

In this section, the protocol is analyzed and some important security requirements are explained.

- Mutual authentication: In the protocol, V1 and V2 are verified by CH to authenticate SNs. Also, SN1 and SN2 verify V4 and V3 respectively to authenticate CH. So all of identities are authenticated successfully.
- Anonymous authentication: Using AID 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 words, a dynamic process is used in the protocol. So adversary cannot trace sensor's activities.
- Fair session key agreement: After sensors' authentication, they should be able to communicate with each other. Due to unsafe channel, it is better to establish a session key at the end of the protocol.
- Scalability: In the protocols, by receiving M1 message, CH first checks the Tri Value with saved records in database. Its response is quick and it does not perform any heavy computations. So our protocol is scalable.
- Availability: In many authentication schemes, updating secret keys increase the probability of de-synchronization attack. In the protocol instead of V_1 (or V_2), we use AV to make scheme available.

V. COMPUTATIONAL COST ANALYSIS AND COMPARISON

In this section, the protocol is compared with previous protocols in terms of security requirements, resistance to different attacks and computational costs. As it is shown in Table II, our scheme can satisfy important features in IoT environments.

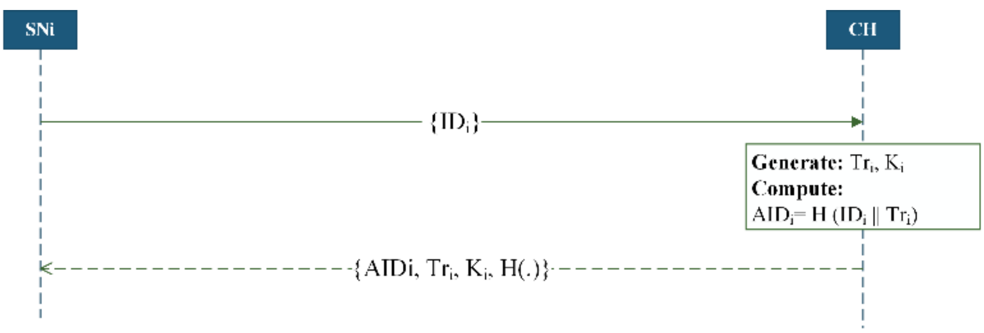

Fig. 2 Registration Phase

International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:13, No:2, 2019

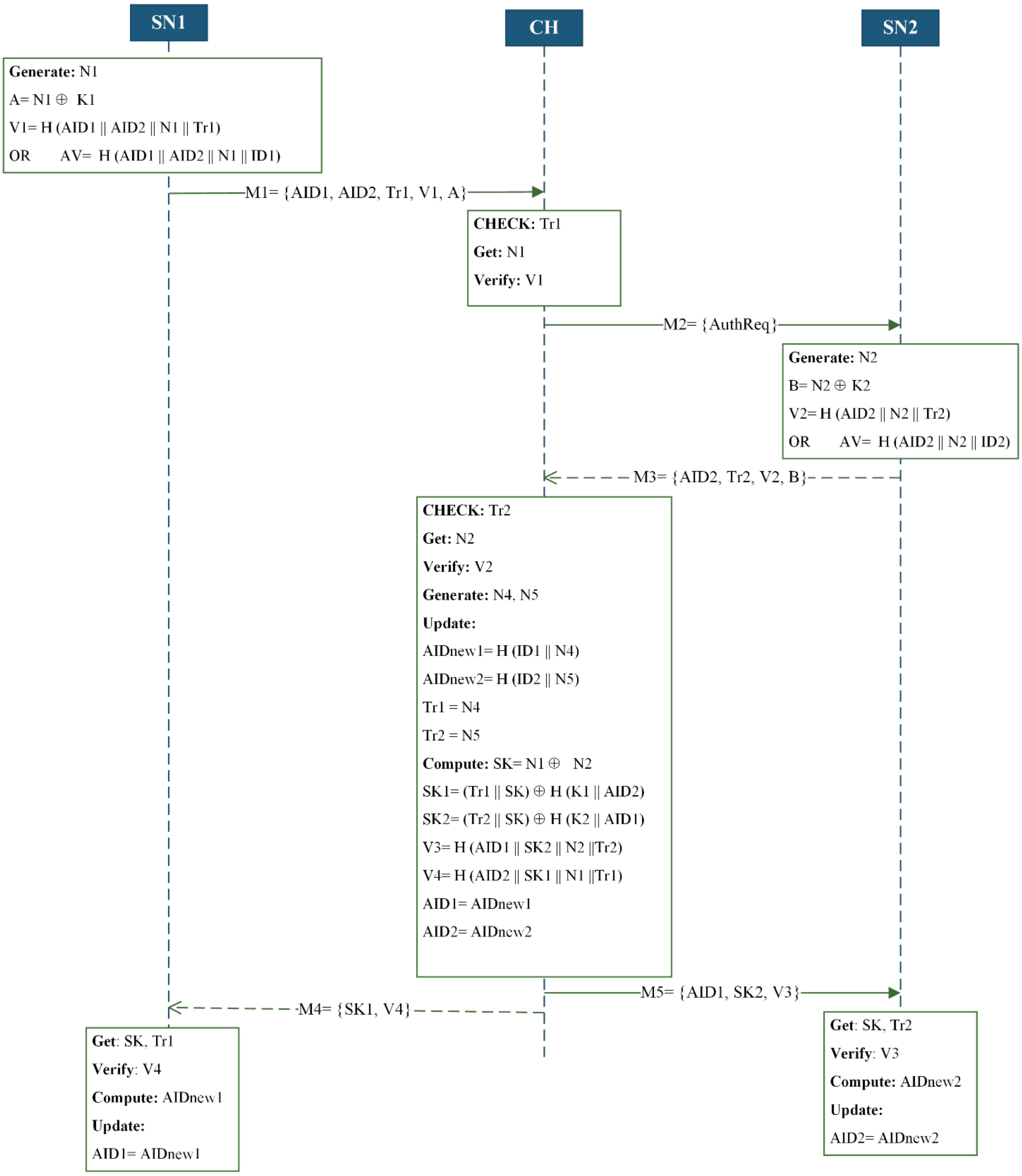

Fig. 3 Proposed protocol for authentication phase

In [14], all features are supported but as it is shown in table III, it is vulnerable against cloning attack but in our protocol, each SN has its own secret keys. If a sensor is captured, adversary cannot get other sensors secret keys. So our scheme can resist this type of attack. In [11] authentication is performed between SN and CH in movement state but it does not support the session key agreement at the end of authentication. Also it is vulnerable against replay attack. In our scheme some random numbers such as Tr_i and N_i are used to verify freshness of statements. So if an adversary tries to intercept and resend messages, it will be detected immediately. Also our scheme can resist impersonation attack. Only legitimate entities can create valid messages. Messages are included secret keys that the attacker does not know. Verifying messages in each step, adding random numbers in statements, checking Tr_i and using AV_i instead of V_i are solutions to resist Man in the middle (MIM), Eavesdropping, DOS and De-synchronization attacks respectively. In addition, the protocol has less computational cost rather than other sensor to sensor authentication schemes. For comparisons of the computational cost, operations execution time are measured based on a modular multiplication operation [17]. Table IV presented these computations.

TABLE II
PERFORMANCE ANALYSIS BASED ON FEATURES

Symbol	R1	R2	R3	R4	R5	R6
[9]	✓	×	×	✓	✓	✓
[14]	✓	✓	✓	✓	✓	✓
[15]	✓	×	×	×	×	×
[11]	✓	✓	✓	×	✓	✓
[13]	✓	×	×	✓	✓	✓
Proposed	✓	✓	✓	✓	✓	✓

R: Requirements; R1: Mutual authentication; R2: anonymity; R3: Untraceablity; R4: Fair session key agreement; R5: Scalability; R6: Availability.

TABLE III
RESISTANCE AGAINST ATTACKS

Symbol	A1	A2	A3	A4	A5	A6	A7
[9]	✓	×	×	×	×	✓	✓
[14]	✓	✓	×	✓	✓	✓	✓
[15]	×	✓	✓	×	✓	×	×
[11]	✓	×	✓	✓	✓	✓	✓
Proposed	✓	✓	✓	✓	✓	✓	✓

A: Attacks; A1: Impersonation; A2: Replay; A3: Cloning; A4: MIM; A5: Eavesdropping; A6: DOS; A7: De-synchronization

TABLE IV
COMPARISON OF COMPUTATIONAL COSTS

Symbol	Computational Cost	Protocol Execution Time
[9]	$2T_{ecm}+T_{eca}+2T_h+2T_{mac}$	≈2406.44 Tmul
[14]	$18T_h + 11T_x + 10T_c$	$\approx 6.48\ T_{mul}$
Proposed	$16T_h + 9T_x + 30T_c$	$\approx 5.76\ T_{mul}$

T_{ecm}: elliptic curve point multiplication operation; T_{eca}: elliptic curve point additon operation; T_h: hash function operation; T_{mul}: modular multiplication operation; T_x: xor operation; T_c: concatenate operation; *due to low computational cost, we ignore T_x and T_c.

VI. CONCLUSION

Different communications between entities are divided into two categories: vertical and horizontal. In this paper, we focus on horizontal and sensor-to-sensor communication. Then mutual authentication protocol between two SNs in IoT environment is presented and analyzed. The protocol satisfies most of the important features such as anonymity, untraceablity, availability and so on. It comprises of two phases: registration phase and authentication phase. In comparison, it is demonstrated that the scheme resists against security attacks and by decreasing computational cost functions, it becomes lighter than previous ones.

REFERENCES

[1] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, pp. 1497-1516, 2012.
[2] K. Ashton, "That 'internet of things' thing," RFiD Journal, vol. 22, pp. 97-114, 2009.
[3] S. H. Shah and I. Yaqoob, "A survey: Internet of Things (IOT) technologies, applications and challenges," in Smart Energy Grid Engineering (SEGE), 2016 IEEE, 2016, pp. 381-385.
[4] 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 Secure Internet of Things (SIoT), 2015 International Workshop on, 2015, pp. 49-57.
[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] J. M. Kizza, "Computer Network Security Protocols," in Guide to Computer Network Security, ed: Springer, 2015, pp. 357-386.
[8] 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.
[9] 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.
[10] 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.
[11] P. Gope and T. Hwang, "Untraceable sensor movement in distributed IoT infrastructure," Sensors Journal, IEEE, vol. 15, pp. 5340-5348, 2015.
[12] 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.
[13] D. A. Ha, K. T. Nguyen, and J. K. Zao, "Efficient authentication of resource-constrained IoT devices based on ECQV implicit certificates and datagram transport layer security protocol," in Proceedings of the Seventh Symposium on Information and Communication Technology, 2016, pp. 173-179.
[14] 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.
[15] K. Srivastava, A. K. Awasthi, S. D. Kaul, and R. Mittal, "A hash based mutual RFID tag authentication protocol in telecare medicine information system," Journal of medical systems, vol. 39, p. 153, 2015.
[16] D.-Z. Sun and J.-D. Zhong, "Cryptanalysis of a Hash Based Mutual RFID Tag Authentication Protocol," Wireless Personal Communications, vol. 91, pp. 1085-1093, 2016.
[17] D. He and S. Zeadally, "An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography," IEEE Internet of Things Journal, vol. 2, pp. 72-83, 2015.