Received March 17, 2019, accepted March 25, 2019, date of publication April 1, 2019, date of current version April 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2908499

Design of a Secure Password-Based Authentication Scheme for M2M Networks in IoT Enabled Cyber-Physical Systems

KM RENUKA[1], SARU KUMARI[1], DONGNING ZHAO[2], AND LI LI[3]
[1]Department of Mathematics, Chaudhary Charan Singh University, Meerut 250001, India
[2]Shenzhen Vetose Technology Co. Ltd., Shenzhen 518102, China
[3]Shenzhen Institute of Information Technology, Shenzhen 518172, China

Corresponding authors: Dongning Zhao (582101@qq.com) and Li Li (lili_hitsz@163.com)

ABSTRACT The Internet of Things (IoT) forms a foundation for cyber-physical systems. We propose an efficient and secure authentication scheme for machine-to-machine (M2M) networks in IoT enabled cyber-physical systems. Smart objects and smart devices over CPS are capable of capturing a variety of multimedia contents; interact with each other and also with the physical world in a fully automatic manner without human interference. The proposed scheme allows any pair of entities in an M2M network to mutually authenticate each other and agree on a session key for communicating data in a secure and efficient way. The authentication process does not incorporate the M2M service provider, and hence eliminates the burden of managing the authentication of massive scale devices at the edge of the network. The burden of the authentication process is offloaded and distributed on the gateways under the authority of this M2M service provider. The proposed scheme requires the mobile user to hold only one secret key provided by the M2M service provider, by which, he can roam randomly in the M2M network and authenticate to any of the gateways in the domain. Then, this authenticated gateway allows the mobile user to authenticate with any sensor node in the domain. In the proposed scheme, the authentication process does not rely on any public key cryptographic operations. Authentication is achieved using very few hash invocations and symmetric key encryptions. Therefore, the scheme is suitable for environmental sensors which are limited in resources (computation, storage, and energy). We analyze the security of the proposed scheme using BAN logic, which is widely accepted as a framework for the assessment of authentication protocols and also using ProVerif. We assess the efficiency of the proposed scheme and compare with some recently proposed schemes.

INDEX TERMS Password authentication, M2M networks, cyber-physical systems, key exchange, mutual authentication.

I. INTRODUCTION

Cyber-physical systems (CPS) are deliberately structured physical systems which are integrated, coordinated, controlled and monitored, through a computational and communication pool. In the digital world, as the Internet governs interaction of humans with one another, analogously CPS is on the verge of governing the human interaction with the physical world. Proliferation of IoT is responsible for the emergence of CPS so that the information from various related perspectives can be monitored and synchronized between physical locations and computational spaces. The Internet of Things (IoT) forms a foundation for cyber-physical systems.

For long distance remote devices (e.g. mobile and sensors), M2M is considered a promising accessing approach for IoT. The world has been made smaller by IoT, however, a gap still exists between our physical world and the cyber world. In the near future, this gap will vanish and all objects in the physical world will be connected to the cyber world by the Cyber-Physical System (CPS). Hence, there will be no longer a distinction between the cyber world and the physical world [1], [2]. Objects and devices over CPS are capable of capturing a variety of multimedia contents, are

The associate editor coordinating the review of this manuscript and approving it for publication was SK Hafizul Islam.

able to exchange information (e.g. locations, states, telemetries, commands, etc.) among each other and also with the physical world in a fully automatic manner without human interference. According to [3], a three-tier CPS consists of three main components. (i) In an environmental tier, there is a group of sensors. (ii) The service tier is formed by a set of actuators. (iii) The controllers forming the control tier. Information is collected by sensors from the physical system. This information is sent to the distributed controllers in the cyber system for processing. Once information is processed, the controllers conduct the actuators to issue the operations commands. Related operations and feedback generation are activated by the actuators to impose on the physical system. Through these operations, CPS is able to accomplish self-awareness, self-adjustments and judgments [4].

M2M communication is the way to implement the function of the environmental tier in CPS. In M2M, sensors and smart/mobile devices communicate with each other utilizing both wired and wireless links. The communication system of an M2M consists of three domains that are interlinked together [5], [1]. As shown in Figure 1, we have, (i) Gateways, representing M2M area domain including M2M area networks. (ii) Communication network domains incorporating wireless and wired networks. (iii) End users and applications required for CPS representing the application service domain.

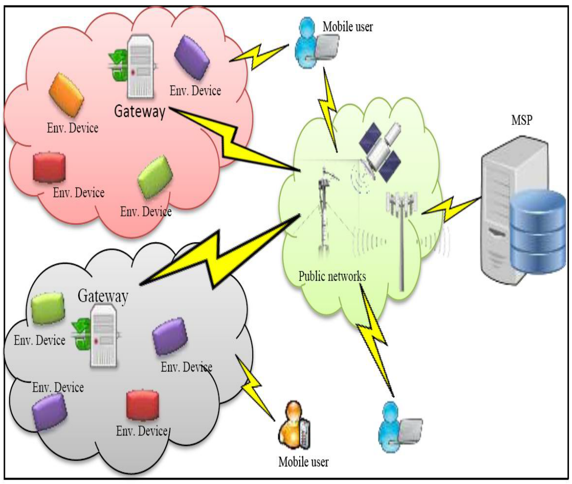


FIGURE 1. M2M Networks in cyber physical systems.

As remote devices/sensors – also called ''environmental devices'' (Env. devices) – are usually found faraway in unattended or forbidden areas, it is likely that the sensors might be hacked by assailants and pirated. For instance, the software might be infused or tainted by specific pernicious codes, which might change or manufacture approaching active information. Also, the sensors might perform self-assertive (Byzantine) rowdiness subsequent to being compromised. Thus, the information sent by remote detecting sensors must be verified. Otherwise, remote beneficiaries on the other side would receive manipulated information and thus react erroneously. The M2M remote/environmental sensors are managed and controlled by an entity called, M2M Service Provider (*MSP*). This entity also conducts registration of the other entities and executes initialization/setup of the system parameters.

In M2M, as the system mainly deals with machines, the authentication strategies are indeed different from conventional authentication. Many existing authentication techniques assume that the entities to be authenticated are humans. Therefore, password (memorable patterns) based authentication and biometric (e.g. fingerprint, voice patterns, etc.) based authentication strategies are not applicable or at least inefficient in the context of M2M authentication.

Our Contribution: This paper contributes to propose an authentication scheme for M2M networks in the CPS system. The scheme is computationally efficient in the sense that, it requires the mobile device and the sensors to perform only very few symmetric encryption/decryption operations and very few hash invocations. And for this reason, the proposed scheme is more suitable for the resource-constrained environment as compared to schemes already presented in the literature as will be depicted during efficiency evaluation. The mobile sensor nodes are not required to perform any public key cryptographic operations. We prove the security of the proposed scheme using the BAN logic framework [6], [7] that is widely accepted for the assessment of authentication protocols. Finally, we evaluate the efficiency of the scheme and compare its performance with related schemes.

Paper Organization: The related work is given in section 2. Section 3 describes the network model, assumptions and threat model. Section 4 is about the description of the proposed scheme. The security of the scheme is analyzed and proved in section 5. The efficiency of our scheme is evaluated in section 6. Comparisons with previous proposals are given in section 7. Finally, the conclusion is in section 8.

II. RELATED WORK

Many authentication schemes such as [8]–[10] have been proposed for different applications. The work in [11] proposed a scheme to filter out bad reports in the M2M system. The scheme is a cooperative authentication scheme which is bandwidth efficient. Although, it well protects against compromising attacks that is undetectable due to the fact that, the compromise occurs when the nodes acquire sleep mode, the scheme does not addresses the protection of the system attacks like impersonation attacks, replay attacks, etc.

In [12], using existing authentication schemes in mobile telecommunication operators, a novel approach has been proposed for automated over-the-air authentication for M2M networks. The implementation of the scheme actually extends the existing standard architecture of generic bootstrapping (GBA), which already exists in the 3G project specifications. The coordinator node derives the required shared keys by authenticating itself to the mobile operator. The subsequent communication between the M2M server and the coordinating node is performed using the shared keys. However, feasibility of the GBA extension is questionable. The work also did not analyze the vulnerability to different attacks in the M2M system.

A healthcare dedicated M2M architecture has been proposed in [13]. The scheme supports hospital applications with the mobility of patients and doctors. They employed ID-based authentication strategies for M2M system. The scheme uses pair wise key pre-distribution for the establishment of a shared key between the sensor node and the mobile sink. It seems that the proposed scheme is able to stand against impersonation attacks due to the employment of dynamic ID's. However, inspections show that the scheme is not able to withstand DoS and replay attacks. Another shortcoming is the easy disclosure of the identities of the mobile and sensor devices. The work in [2] did not aim at devising a particular scheme. They adopted a rigor and formal model in the theory of cryptography in an attempt to construct a generic framework for the analysis of the security and functionality of M2M authentication schemes. Four adversarial models were proposed to tackle different attacks. However, the framework lacks the details of any specific authentication scheme, any specific application and the corresponding attacks. The contribution of [14] focuses mostly on withstanding man-in-the-middle attack. The protocol protects the information privacy of other machines and users that are not the subjects of the communication.

Recently, in [1], ID-based cryptosystems were employed, combined with key exchange strategies, in particular, the Authenticated Identity-Based Cryptography (IBC) without Key-Escrow (AIBCwKE) mechanism. The scheme seems to withstand most of the known attacks; however, the scheme requires the target sensors and mobile devices to perform computationally expensive cryptographic operations. It requires a sensor to perform several bilinear pairing operations on elliptic curves in addition to several point multiplications and exponentiations. These computation requirements are not adequate for devices with very limited resources. The proposed scheme does not rely on any PKI. The proposed scheme can authenticate any pair of devices in an M2M site using only few symmetric encryptions/decryptions and few invocations of a hash function. These computations are extremely lightweight compared to other ID-based cryptosystems which require computationally expensive cryptographic operations on elliptic curves.

III. ASSUMPTIONS, DESCRIPTION AND MODEL

As depicted in Figure 2, the four main entities of the proposed scheme are as follows: (i) M2M service provider (*MSP*), it conducts registration of the other entities and executes initialization/setup of the system parameters. (ii) Environmental devices or sensors, which are very limited in resources (computation, storage and energy). (iii) Mobile devices which have limited energy resources although are richer at resources as compared to environmental sensors. (iv) Gateways, which are the pivot of all the authentication protocols between any pair of devices. There is at least one gateway in every M2M site. Some of the sensors are directly connected to the gateway while others may connect indirectly through another connected sensor or a mobile device after authenticating with the gateway. The *MSP* is considered to be trustworthy for obvious reasons as it is authorized for generating all the secret parameters required by the system. All other entities may behave maliciously.

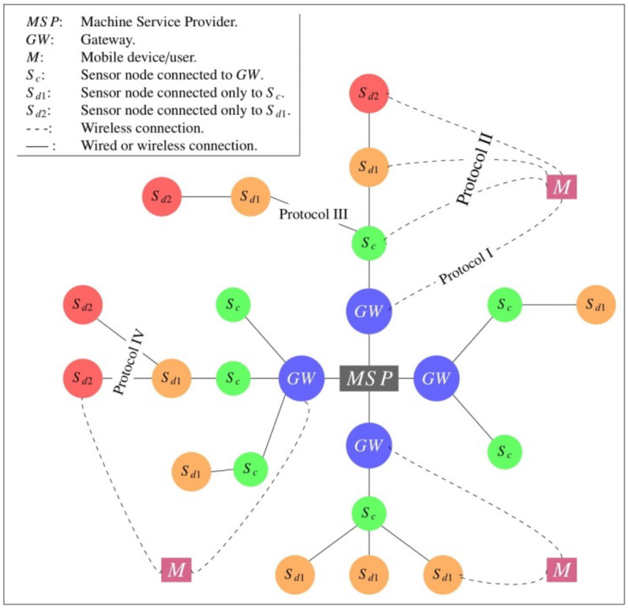


FIGURE 2. M2M Network architecture for the proposed scheme.

The proposed scheme requires a mobile user to contact the *MSP* only once to register his identity and obtain a long-term master secret key of sufficiently long bit-length. Later, without the incorporation of the MSP, the mobile user, roaming randomly in the M2M network (using this master secret key) is able to mutually authenticate with any of the gateways under the authority of the MSP. Once a user authenticates with any of the gateways, he is able to mutually authenticate with any of the sensors registered on this gateway. Moreover, the sensors are not necessarily required to be connected to the gateway at the time of authentication. Also, the scheme allows any two sensors in the M2M network to mutually authenticate and exchange data. After system initialization and registration of all entities, the authentication phase of the scheme between any two sensors/devices does not incorporate the MSP and consists mainly of four protocols:

- Protocol I: Allows the mobile device (using its master secret key) to mutually authenticate with any gateway.
- Protocol II: Given that protocol I was executed successfully between a mobile user and the gateway. The mobile user, with the help of the gateway, is able to mutually authenticate with any of the sensors within the domain of this gateway.
- Protocol III: Allows any two sensors, where at least one of them is connected to a gateway, to establish an authenticated channel between each other.

- Protocol IV: Allows any two sensors disconnected from the gateway to establish an authenticated channel. This is accomplished with the help of another sensor that is connected to the gateway.

Threat model: Following three varieties of adversaries are considered for the proposed scheme:

(i)*Outsider adversary:* This adversary is capable to eavesdrop on all possible communication links in the system. It can record as well as replay messages to any party involved in the communication. It can decompose as well as reassemble an eavesdropped message (plaintext/cipher text) into a new message to resend it to any of the legal participating entity. It can use the compromised secret keys for decryption and interpretation of the encrypted messages.

1. **Device corruption adversary:** It has all capabilities that an outsider adversary possesses. Further, it can utilize the secret key shared on the device for decrypting/forging the eavesdropped messages. Thus, it fully controls the captured device.
2. ***MSP* corruption adversary:** Along with the capabilities that an outsider adversary possesses, it can also steal/manipulate *MSP* database system.

IV. DETAILED DESCRIPTION OF THE PROPOSED SCHEME

The scheme follows the M2M architecture given in Figure 2. There is an M2M service provider (*MSP*) and a set of gateways under the authority of this *MSP*. Each gateway is connected to a set of sensors. There is also a set of mobile users. At any time, a user may want to authenticate with any of the gateways he/she authorized for (by the *MSP*). Also, the user may want to authenticate with any of the sensors to monitor/collect information. Finally, we assume that any two sensors may want to authenticate each other for the purpose of communicating data. The important notations used in the scheme are shown in Table 1.

A. INITIALIZATION PHASE

- The *MSP* has its own public/private key pair (pk_{MSP}, sk_{MSP}) of a digital signature algorithm for authentication purposes with her gateways (GW). The public key pk_{MSP} is stored on each GW under the authority of *MSP*.
- The *MSP* generates a public/private key pair (pk_{GW}, sk_{GW}) for each GW. The *MSP* stores pk_{GW} for each GW, while sk_{GW} is stored on the corresponding GW. We emphasize that these public keys are used only in the registration process between the MSP and her gateways. The authentication phase is irrelevant to these public keys.
- The *MSP* assigns a unique identity ID_{GW} for each GW.
- The M2M network administrator installs a shared master secret key on the GW and each of the sensors (S) in the domain. Thus, each sensor S shares a random unique master secret key $k_{GW}^{(S)}$ with the GW. Also, each sensor S knows the identity ID_{GW} while the GW knows the identities ID_S of the sensors in the domain.

TABLE 1. Notations used in the proposed protocol.

Notations	Meaning
MSP	M2M service provider
GW, M	Gateway, Mobile user
$s/s_c/s_d$	Sensor node/connected to GW/disconnected from GW
ID_X, PW_M	Identity of entity X, Password of M
$k_X^{(Y)}$	Secret key shared between entities X and Y
r_X	Random nonce picked by entity X
(pk_{MSP}, sk_{MSP})	Key pair of MSP: (Public, Private)
(pk_{GW}, sk_{GW})	Key pair of GW: (Public, Private)
$E_k(x)$	Use of key k to encrypt a value x
$H(x)$	Computing hash of a value x
$\oplus$	Bitwise XOR operator
$\|$	String concatenation operator
$X \rightarrow Y$	X computes and sends to Y

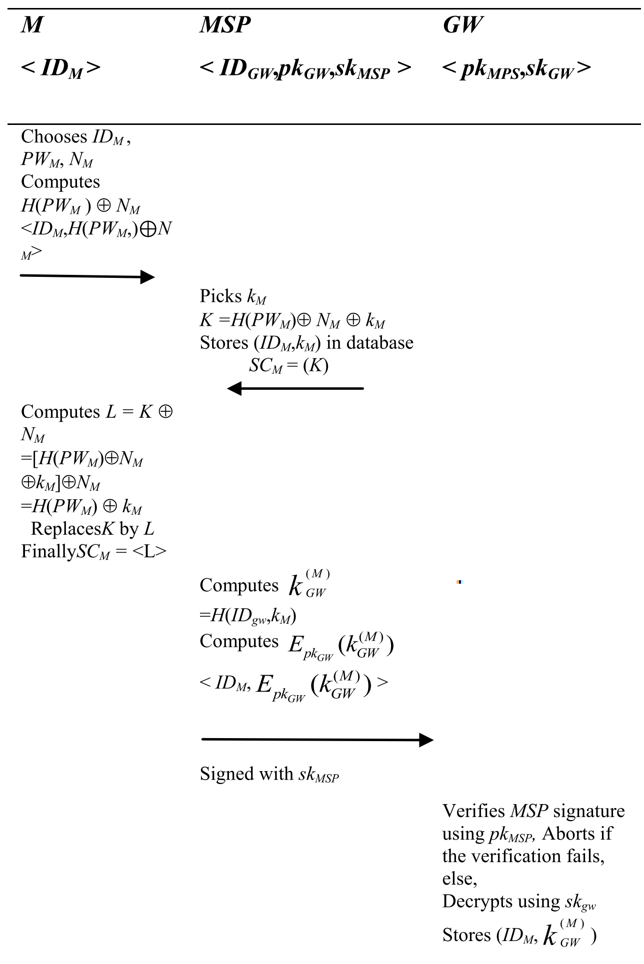


FIGURE 3. The registration phase of the proposed scheme.

B. MOBILE USER REGISTRATION OVER A SECURE CHANNEL

The registration phase is illustrated in Figure 3.

Over a secure channel, a mobile user M approaches the MSP with his chosen identity ID_M and password PW_M. MSP determines the identities, ID_{GW} of the gateways that this user is authorized for and wants to communicate with. The user registers as follows:

1. $M \rightarrow MSP$: M chooses a random number N_M, computes $H(PW_M) \oplus N_M$. Sends $(ID_M, H(PW_M) \oplus N_M)$ to *MSP*.
2. $MSP \rightarrow M$: Picks k_M as master key for M and computes $K = H(PW_M) \oplus N_M \oplus k_M$. Stores K in M's smartcard $SC_M = \{K\}$. *MSP*stores $\{ID_M, k_M\}$ with itself in its database and sends the smartcard $SC_M = < k >$ to M.
3. M: On receiving $SC_M = \{K = H(PW_M) \oplus N_M \oplus k_M\}$, M inserts the smartcard into the card reader and inputs ID_M, PW_M and N_M. Smartcard computes $L = K \oplus N_M = [H(PW_M) \oplus N_M \oplus k_M] \oplus N_M = H(PW_M) \oplus k_M$. M discards K and stores L in the smartcard so that $SC_M = \{L = H(PW_M) \oplus k_M\}$.
4. $MSP \rightarrow GW$: Computes $k_{GW}^{(M)} = H(ID_{GW}, k_M)$. Sends $(E_{pk_{GW}}(k_{GW}^{(M)}), ID_M)$, signed with sk_{MSP}
5. GW: Verifies *MSP* signature using pk_{MSP}. Decrypts $(E_{pk_{GW}}(k_{GW}^{(M)})$ using sk_{GW} Stores the tuple $<ID_M, k_{GW}^{(M)}>$

This finalizes the registration phase. The *MSP* stores the identities of all the mobile users and gateways and the users k_M in a secure database. The user M stores the tuple $<ID_{GW}, k_M>$ in his smartcard. The GW stores $<ID_m, k_{GW}^{(M)}>$ for each user M.

C. PROTOCOL I: MOBILE-GATEWAY AUTHENTICATION

The mobile user M must first authenticate itself to the gateway $GW$and establishes a session key for data transfer. The protocol is illustrated in Figure 4 and operates as follows:

1. $M \rightarrow GW$:
   - Picks a random nonce r_M.
   - Sends (broadcasts) the tuple, (*Hello GW,* ID_M, r_M).
2. $GW \rightarrow M$:
   - Checks that ID_M exists and fetches the corresponding $k_{GW}^{(M)}$
   - Picks a random nonce r_{GW}
   - Computes $E_{k_{GW}^{(M)}}(r_M, r_{GW})$. Sends the tuple, $< ID_{GW}, ID_M, E_{k_{GW}^{(M)}}(r_M, r_{GW}) >$
3. M → GW :
   - Retrieves his master key $k_M = L \oplus H(PW_M)$ and using k_M and the received ID_{GW}, locally computes $k_{GW}^{(M)} = H(ID_{GW}, k_M)$
   - Using $k_{GW}^{(M)}$, decrypts for r_M and r_{GW}
   - Checks r_M with the received value. Aborts if r_M is not valid, else,
   - Picks k_s as a session key.
   - Computes the symmetric encryption $E_{k_{GW}^{(M)}}(r_{GW}, k_S)$.
   - Sends $< ID_M, ID_{GW}, E_{k_{GW}^{(M)}}(r_{GW}, k_S) >$
4. GW:
   - Using $k_{GW}^{(M)}$, decrypts for r_{GW} and k_s. Checks r_{GW}. Aborts if r_{GW} is not valid, else, accept k_s as a session key.

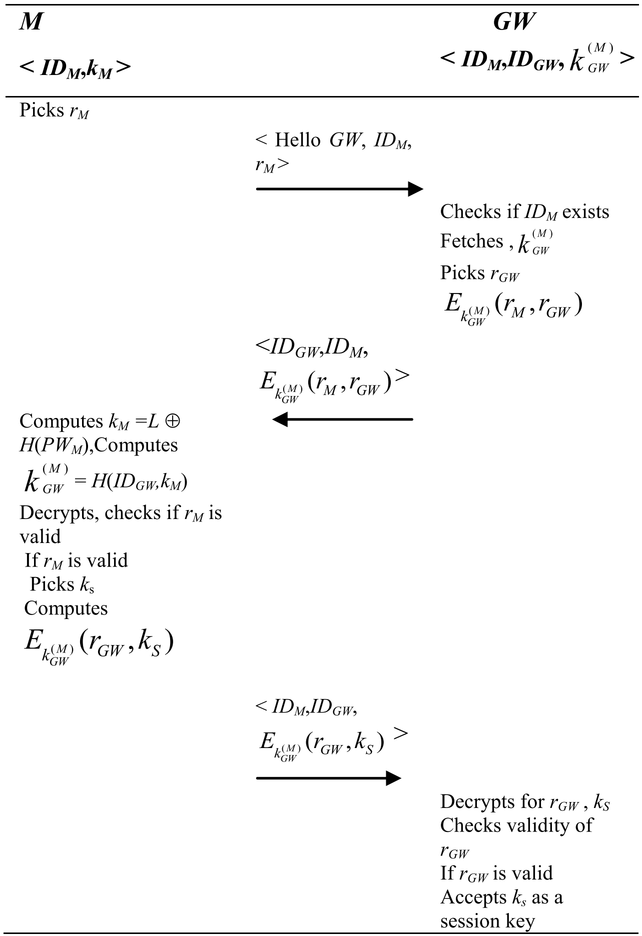


FIGURE 4. Protocol-I: Mobile-Gateway authentication.

D. PROTOCOLII: MOBILE-SENSOR AUTHENTICATION

Recall that, GW shares a master secret key $k_{GW}^{(S)}$ with each sensor node in the domain. Also, recall that the user M shares a secret key $k_{GW}^{(M)}$ with the GW he already authenticated in Protocol I. Notice that M shares nothing with any of the sensors. We assume that M knows the identity of each sensor, *IDs*we assume that, *GW*is always reachable by *M,* while the sensor may not be able to reach *GW.* This situation is common, for example, if the sensor is a moving sensor that may reach a distance out-ranging the gateway.

In the following we give the description of the authentication protocol to allow different M2M sensors which may or may not be connected to the gateway at the time of authentication, to authenticate with a user M with the help of the gateway *GW.* The user M's device is the device guaranteed to be connected to the gateway (e.g. via WiFi, Zigbee, over a GPRS, GSM, etc.). Protocol II sequence diagram is shown in Figure 5 and described next.

1. $M \rightarrow S :< ID_M, ID_S >$.
   M, sends a tuple including its identity ID_M,the identity of the target sensor, ID_S.
2. $S \rightarrow M$: $<(IDs, ID_M, E_{k_{GW}^{(S)}}(ID_M, IDs, r_s) >$

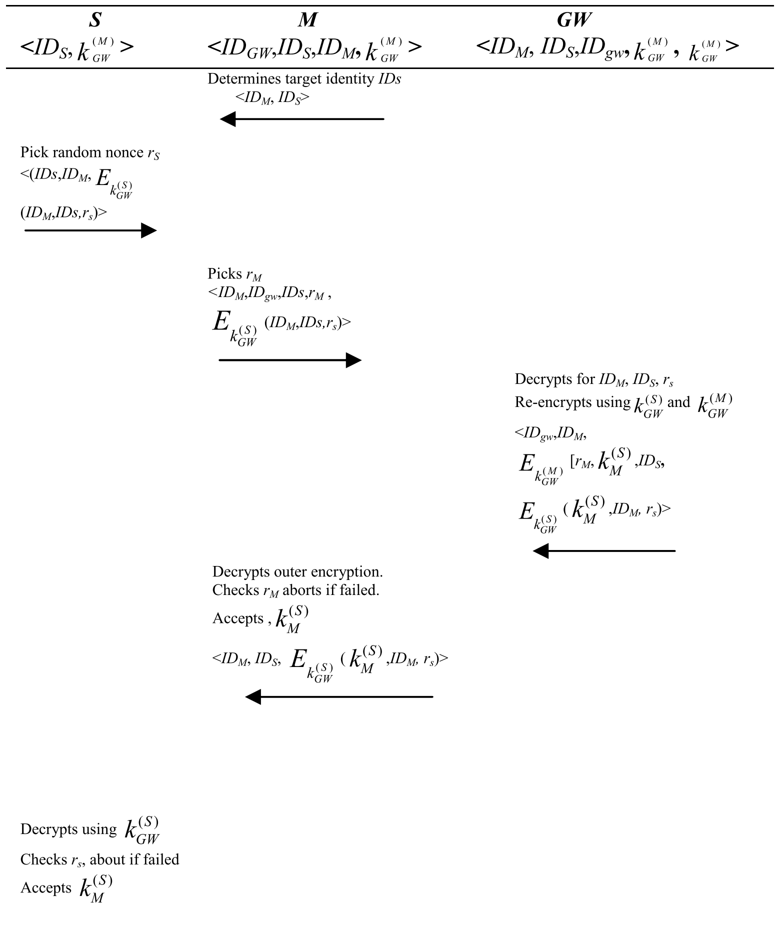


FIGURE 5. **Protocol-II: Mobile-Sensor authentication.**

Once the message in step one reaches S, S replies with a message encrypted with the pre-shared key $k_{GW}^{(S)}$ to M, which contains the identity of M, ID_M identity of S, IDs and $S's$ random nonce r_S generated by sensor S

3. $M \rightarrow GW$: $< ID_M, ID_{gw}, IDs, r_M, E_{k_{GW}^{(S)}}(ID_M, IDs, r_s) >$
   M forwards the encryption it received from S to the GW, side by side with a random nonce r_M generated by him. Notice that ID_S must be sent in the clear to tell GW which secret key $k_{GW}^{(S)}$ to use.
4. GW→M:
   $<ID_{GW}, ID_M, E_{k_{GW}^{(M)}}[r_M, k_M^{(S)}, ID_S E_{k_{GW}^{(S)}}(k_M^{(S)}, ID_M, r_s) >$
   The GW prepares an encapsulated encryption. The outer encryption is dedicated for M including the nonce r_M for authenticating the GW to M and the new session key $k_M^{(S)}$ between M and S, picked by GW. The inner encryption is dedicated for S including the nonce r_S for authenticating GW to S and the same session key between M and S.
5. $M \rightarrow S$: $<ID_M, ID_S, E_{k_{GW}^{(S)}}(k_M^{(S)}, ID_M, r_s) >$
   M decrypts the outer encryption, verifies the nonce r_M, if correct, stores $k_M^{(S)}$ as the session key. He forwards the inner encryption as it is to S. S decrypts, verifies the nonce r_S, if correct, stores $k_M^{(S)}$ as the session key for this mobile device M.

E. SENSOR-TO-SENSOR AUTHENTICATION

Two sensors S_c and S_d(the subscript c stands for "Connected to GW" while d stands for "Disconnected from GW") in an M2M domain, each share a common key $k_{GW}^{(S_c)}$ and $k_{GW}^{(S_d)}$ $k_{GW}^{(S_d)}$ respectively with GW, want to communicate with each other or with the gateway GW. We assume the general case, that only one sensor is reachable by the GW. Here, we have two different scenarios, each require a different protocol:

•**Protocol III.** One sensor node, say S_d, wants to communicate with the GW, however, S_d is out-ranging GW and the only way to establish a connection is through S_c which is connected to the GW.

•**Protocol IV.** S_{d1} and S_{d2} are both out-ranging the GW. However, one of them is connected to S_c, which is connected to the GW. S_{d1} and S_{d2} want to mutually authenticate with each other to exchange data. The connected node S_c will help them to establish a session key, $k_{S_{d1}}^{(S_{d2})} k_{S_c}^{(S_d)}$

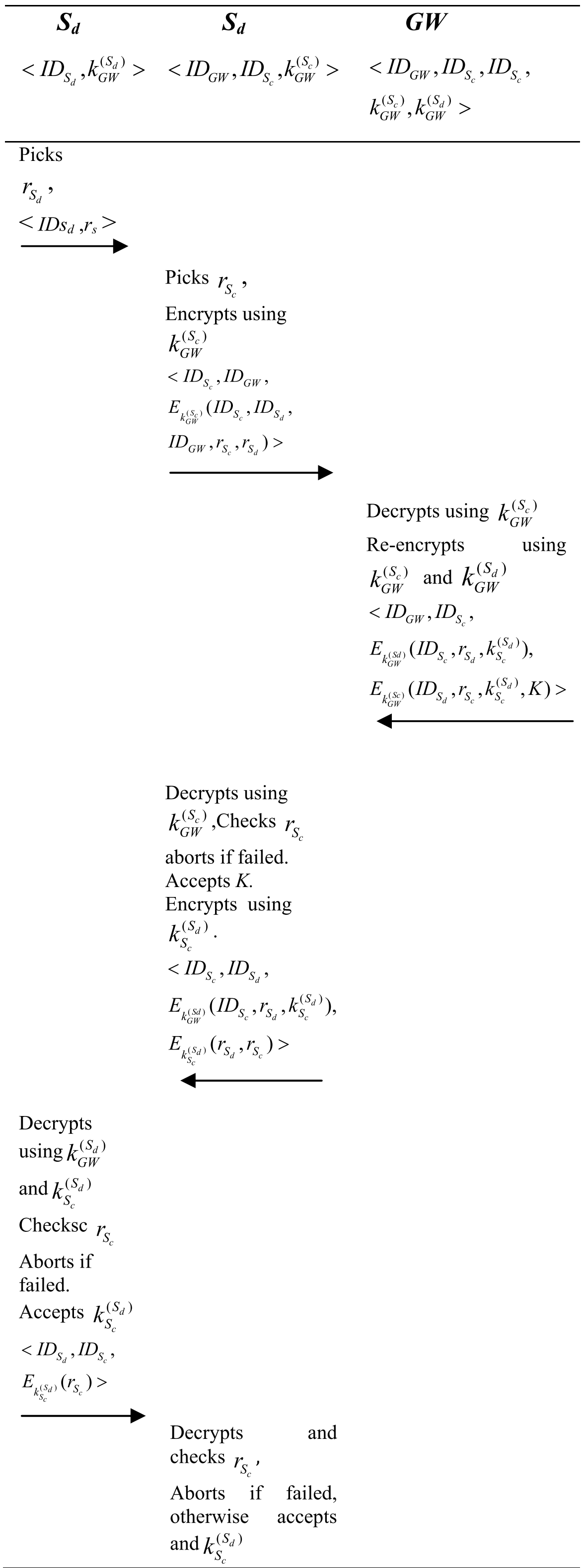


FIGURE 6. **Protocol-III: Sensor-to-Sensor authentication.**

1) PROTOCOL III

We assume S_d is out-ranging *GW*, while S_c is connected to both S_d and *GW*. In this case, the protocol allows the establishment of a session key, $k_{S_c}^{(S_d)}$ between S_c and S_d and also a session key *K* between *GW*and S_c so that, the link " S_d- S_c-*GW*" becomes fully authenticated and private. The protocol is illustrated in Figure 6 and is as follows:

1. S_d: broadcasts the tuple, $< IDs_d, r_s >$
   Sensor node S_d, broadcasts a request for connection including its own identity IDs_d and a random nonce r_{S_d} picked by herself. After receiving the broadcasted message/tuple, node S_c (and other nodes connected to *GW* that receive the message) send the tuple in step (2) below.
2. S_c:→*GW*
   $< ID_{S_c}, ID_{GW}, E_{k_{GW}^{(S_c)}}(ID_{S_c}, ID_{S_d}, ID_{GW}, r_{S_c}, r_{S_d}) >$
   S_c sends a message encrypted with the pre-shared key $k_{GW}^{(S_c)}$ to *GW*, which contains identity IDs_d, and random nonce r_{S_d} identity ID_{S_c} and random nonce r_{S_c} generated by node S_c. *GW* decrypts the messages using the pre-shared key. *GW* recognizes that sensor node S_d is the node that want to authenticate with *GW*. *GW* then determines the most suitable sensor node to be connected with S_d and sends the tuple in step (3) to the right node (assumed S_c) as a reply, meanwhile *GW* sends a termination message to other nodes to inform them that their cooperation is no longer needed.
3. *GW* → S_c:
   $< ID_{GW}, ID_{S_c} E_{k_{GW}^{(Sd)}}(ID_{S_c}, r_{S_d}, k_{S_c}^{(S_d)})$
   $, E_{k_{GW}^{(Sc)}}(ID_{S_d}, r_{S_c}, k_{S_c}^{(S_d)}, K) >$
   This tuple involves $ID_{S_c}, r_{S_d}, k_{S_c}^{(S_d)}$ encrypted with with $k_{GW}^{(S_d)}$ and $ID_{S_c}, r_{S_d}, k_{S_c}^{(S_d)}$, *K* encrypted with $k_{GW}^{(S_d)}$.Included in these encryptions, the session key with $k_{S_c}^{(S_d)}$ Picked by *GW* for S_c and S_d and *K* as the session key between S_c and *GW* picked by *GW* for this session. Now S_c decrypts the message with with $k_{GW}^{(S_c)}$ and gets the session key *K* and with $k_{S_c}^{(S_d)}$ then encrypts the nonce , r_{S_d}, r_{S_d} with $k_{S_c}^{(S_d)}$, and forwards them to S_d together with the other encryption (dedicated to S_d, from *GW*) as shown in step (4)).
4. S_c → S_d:
   $< ID_{S_c}, ID_{S_d}, E_{k_{GW}^{(Sd)}}(ID_{S_c}, r_{S_d}, k_{S_c}^{(S_d)}), E_{k_{S_c}^{(Sd)}}(r_{S_d}, r_{S_c}) >$
   On the reception, S_d decrypts the first encryption to obtain $k_{S_c}^{(S_d)}$, by which, S_d decrypts the second encryption the to obtain both nonces. S_d verifies the correctness of the nonce r_{S_d} and uses, r_{S_c} to confirm to S_c in the next final step.
5. S_d → S_c : $< ID_{S_d}, ID_{S_c}, E_{k_{S_c}^{(S_d)}}(r_{S_c}) >$
   S_c now believes that S_d knows the key $k_{S_c}^{(S_d)}$.

2) PROTOCOL IV

In this protocol, the two sensor nodes S_{d1} and S_{d2} do not share any keys with each other, and are disconnected form *GW*, yet, each node share a master key
$k_{GW}^{(S_{d1})}$. with *GW*. The protocol allows both nodes to authenticate and establish a session key with each other. At least one node (S_{d1} is connected to a third node S_c. This S_c is connected

to GW and shares a master key $k_{GW}^{(S_c)}$ with GW. The protocol is as follows:

1. $S_{d1} \rightarrow S_{d2}$: $< ID_{S_{d2}}, ID_{S_{d1}}, > S_{d2}$ broadcasts a request for authentication with node S_{d1}.
2. S_{d1}, S_c and GW, run **Protocol III,** where S_{d1} play the role of S_d At the end of this protocol, S_{d1} and S_c share a common session key $k_{S_c}^{(S_{d1})}$.
3. S_{d2}, S_{d1} and S_c, run **protocol III,** where S_c plays the role of GW, S_{d2} plays the role of S_c (in protocol III) and S_{d2} plays the role of S_d. At the end, S_{d2} and S_{d1} establish a session key $k_{S_{d1}}^{(S_{d2})}$.

V. SECURITY ANALYSIS

In this section, we assess the security of the proposed scheme. The assessment is based on the basic security requirements, informal discussion on resistance to general attacks, formal security proof using the well-known BAN logic framework.

A. BASIC SECURITY REQUIREMENTS

In the following, we show that the proposed scheme realizes the basic security requirements.

1) MUTUAL AUTHENTICATION

Mutual Authentication in Protocol I, between M and GW is attained as both can deduce M-GW secret key $k_{GW}^{(M)} = H(ID_{GW}, k_M)$ which is used to encrypt/decrypt for the session key k_s. The session key k_s cannot coincide at M and GW so far the encryption and decryption are executed with the same secret key $k_{GW}^{(M)}$ The mobile user M produces $k_{GW}^{(M)}$ at its end with its master secret key k_M and identity ID_{GW} of the gateway. Similarly, MSP has generated $k_{GW}^{(M)}$ and provided it securely to the GW. Thus, if a GW identity ID_{GW} is claimed without knowing $k_{GW}^{(M)}$, this GW cannot be authenticated by a valid user. Further, a mobile user without possessing correct K_M matching with ID_M stored in the database of GW, will not be validated by the GW.

In protocol II, both M and GW have already authenticated each other agreed on the shared secret key $k_{GW}^{(M)}$. Also the sensor node S already shares a secret key $k_{GW}^{(S)}$.GW is the pivot entity to allow both M and S to share a session key $k_{GW}^{(M)}$. Once M requests a connection with S, S replies with the encryption $E_{k_{GW}^{(S)}}(ID_M, ID_S, r_S)$ dedicated to GW, so M forwards the encryption to GW with his random nonce r_M. This encryption contthe random nonce r_s that can be seen only by GW and which will be verified later by S. GW replies with the encapsulated encryption encryption $E_{k_{GW}^{(M)}}$ $[r_M, k_M^{(S)}, ID_S, E_{k_M^{(S)}}(k_M^{(S)}, ID_M, r_S)]$ which delivers $k_{GW}^{(M)}$ to both M and S and also the random nonces for verification.

Protocol III is a modification of protocol II, in the sense that, the sensor disconnected from GW in the entity that requests the connection with the sensor connected to GW. Each sensor shares a secret key with GW. The mutual authentication follows from protocol II. The mutual authentication follows for protocol IV as well.

2) CONFIDENTIAL COMMUNICATION SESSION

In each of the proposed protocols, the shared session key is confirmed by both the participants prior to indulge in any subsequent communication. Only the legitimate participants and GW have knowledge of the master secret keys required for encryption/decryption of the session key. Hence, the scheme maintains the confidentiality of communication.

3) LOW COMPUTATION AND STORAGE COST

The proposed scheme does not involve any public key computations by any entity during the authentication protocols. Only few symmetric encryptions/decryptions and hash invocations are required. Further, the scheme necessitates the mobile user as well as the sensor nodes to store few short identities and one master secret key. Therefore, the proposed scheme is efficiently and easily implementable on smartcards and sensors with very limited resources. Therefore, the proposed scheme exhibits quite low computation and storage costs.

4) PROTECTION OF GW-M AND GW-S KEY

The authentication protocol I treats $k_{GW}^{(M)}$ as a master key in the sense that, this key is never used to encrypt plaintexts that are not random. Notice that, the plaintext encrypted by $k_{GW}^{(M)}$ always contains r_{GW} as a random nonce that is never sent over the public channel and is totally unknown to an eavesdropper. This protects $k_{GW}^{(M)}$ from known plaintext attacks. An inspection of protocols II, III and IV shows that the same protection is attained for the master keys $k_{GW}^{(S)}$ shared between the GW and any sensor S.

5) SESSION INDEPENDENCE

In the proposed scheme, the previous session keys do not contribute to the deduction of fresh session keys, meaning thereby, no relationship among the previous and fresh session keys. Every time, a fresh random string is to serve as a session key. For this reason, leakage of one session key has no affect on other past/future sessions for any pair of entities.

B. PROTECTION OF MOBILE USER'S MASTER KEY K_M

The master key k_M of M is protected with M's password inside the smartcard/mobile device as it is stored as $L = H(PW_M) \oplus k_M$. Further, the master key k_M is used only to generate the keys $k_{GW}^{(M)}$ though the hash invocation $k_{GW}^{(M)} = H(ID_{GW}, k_M)$ which A compromise of $k_{GW}^{(M)}$ allows the attacker to perform brute force attack as an attempt to reach k_M, Since k_M is used only as an input to a hash function, its bit-length is not constrained (e.g. is not limited to the required length of a block cipher key.). Therefore, the MSP freely set this master key sufficiently long to withstand brute force in case any GW is compromised.

C. ATTACKS AND COUNTERMEASURES

We informally discuss how the proposed scheme withstands different types of adversarial attacks described in the threat model.

1) ROGUE GATEWAY

When an adversary corrupts/compromises a gateway GW, then it knows all the secret parameters stored on this GW: $k_{GW}^{(M)}, k_{GW}^{(S)}$ and sk_{GW}. We give emphasis to the following.

- *This compromise does not leads to security-breach of k_M, the master secret key of any mobile user M, provided the hash function used possesses strong one-way property and that k_M is with long enough bit- length.*
- *Compromising the gateway GW does not allow the adversary to deduce any other M-GW secret keys on any other gateway. This follows from the fact that, the M - GW keys are produced independently by applying a one – way hash function on k_M and ID_{GW}, since k_M is unknown to the adversary.*

The countermeasure for a GW compromise is as follows: Firstly, the corrupted GW is cleaned (scanned, rebooted, etc.) with a new public/private key pair pk_{GW}, sk_{GW}, then the MSP selects a new identity, say ID'_{GW}, specifically for this gateway and re-generates new set of M-GW secret keys, $\{k_{GW}^{'(M_1)} \ldots\ldots, k_{GW}^{'(M_m)}\}$ where $k_{GW}^{'(M_j)} = H(ID'_{GW}, k_{M_j})$. Afterwards, the MSP securely provides these secret keys to GW as discussed during the registration phase. Mobile users are informed publically about the rogue identity ID_{GW}. Finally, the system administrator reinstalls new fresh master secret keys $k_{GW}^{(S)}$. for each sensors S in the domain of this GW.

2) ROGUE SENSOR NODE

The only secret stored at the sensor node S is its master secret key which is shared with the GW. This key was chosen at random and installed by the system administrator independently. So, the countermeasure against adversarial knowledge of this key is as easy as installing a new shared key $k_{GW}^{(S)}$ on this sensor and on the gateway. If a sensor node becomes completely rogue and physically captured by the adversary, then the system administrator simply deletes the shared key $k_{GW}^{(S)}$ from the gateway.

3) COMPROMISED MOBILE DEVICE

To reduce the risk of such an attack, the master secret key k_M of a mobile user is required to be stored on a secure tamper proof device. However, still there is a chance for the adversary to compromise this key. Compromise of the master secret key k_M of a mobile user M, does not affect other mobile users. Nevertheless, M must report to the MSP of its compromised master secret key k_M and must ask for revocation of k_M and registration of a new one. In this case, the MSP picks a new master key for M and then generates a new set of GW-M keys, $k_{GW}^{(M)} = H\ (ID_{GW}, k_M)$ and sends them to the gateways.

4) STOLEN MOBILE DEVICE/SMARTCARD

If the user's device is stolen by an attacker, he/she will not be able to procure the master secret key $k_{M.}$ of M. The master key k_M of M is protected with M's password inside the smartcard/mobile device as it is stored as $L = H\ (PW_M\ )\ \oplus\ k_M$. Thus, even if an attacker happens to extract L stored inside the smartcard/mobile device of M, he/she cannot retrieve k_M as the attacker does not know the password of M.

5) MSP DATABASE COMPROMISE

An attacker may find his way to the MSP database servers to disclose the user's master keys. A counter measure against such attack is that, the MSP stores all users' master encrypted under the MSP master key. The MSP master key is then stored on a tamperproof device away from form the database. In this case, stealing the MSP database becomes user less.

6) MAN-IN-THE-MIDDLE ATTACK

Suppose an adversary puts itself as an intermediate node between any two communicating entities. This adversary does not know the master secret keys of this pair of entities. Certainly, the adversary would try to impersonate each entity to the other entity. But, as the adversary is unknown of any of the master secret keys, she is unable to convince any of the entities that she is the other entity. She is unable to generate any correct hashes or encryptions. So, this attack fails.

D. FORMAL SECURITY PROOFS

Now follows, the security of the proposed protocols using the BAN logic.

Lemma 1: Assuming E and H used in protocol I are secure pseudo-random function families, then protocol I utilizing E and H is a secure mutual entity authentication and key exchange protocol.

Proof: Given that H is a strong hash function and that k_M is sufficiently long master secret key for M. A compromise of any $k_{GW}^{(M)} = \mathrm{H}\ (ID_{GW}\ , k_M)$ does not allow a computationally bounded adversary to reach k_M. Now given that both GW and M believe in $k_{GW}^{(M)}$, we continue the proof of this Lemma using BAN logic as follows:

Idealization. The idealized messages between M and GW in protocol I are as follows:

- M1: $M \rightarrow GW$:-
- M2: $GW \rightarrow M$: $\{(r_M, r_{GW})\}_{k_{GW}^{(M)}}$
- M3: $M \rightarrow GW$: $\{(r_{GW}, M \stackrel{k_s}{\longleftrightarrow} GW)\}_{k_{GW}^{(M)}}$

Assumptions.

- A1:$M| \equiv \#(r_M)$
- A2: $GW| \equiv \#(r_{GW})$
- A3:$M| \equiv M \stackrel{k_{GW}^{(M)}}{\longleftrightarrow} GW$
- A4: $GW| \equiv GW \stackrel{k_{GW}^{(M)}}{\longleftrightarrow} M$
- A5: $GW| \equiv M => M \stackrel{k_s}{\longleftrightarrow} GW$
- A6: $M| \equiv M \stackrel{k_s}{\longleftrightarrow} GW$

Main goals.

- G1: $GW| \equiv M \stackrel{k_s}{\longleftrightarrow} GW$
- G2: $GW| \equiv M |\equiv M \stackrel{k_s}{\longleftrightarrow} GW$
- G3: $GW| \equiv M| \equiv r_{GW}$
- G4: $M| \equiv GW| \equiv r_M$

Analysis.

- From A1, A3 and M2, we have,

$\frac{M|\equiv\#(r_M)}{M|\equiv\#(r_M, r_{GW})}$ (Freshness rule)

$\frac{M|\equiv M \xleftrightarrow{k_{GW}^{(M)}} GW, M \triangleleft \{(r_M, r_{GW})\}_{k_{GW}^{(M)}}}{M|\equiv GW|\sim(r_M, r_{GW})}$ (Message meaning rule)

$\frac{M|\equiv\#(r_M, r_{GW}), M|\equiv GW|\sim(r_M, r_{GW})}{M|\equiv GW|\equiv(r_M, r_{GW})}$ (Nonce verification rule)

$\frac{M|\equiv GW|\equiv(r_M, r_{GW})}{M|\equiv GW|\equiv r_M}$ (Belief rule)

Thus, goal G4 is satisfied.

- From A2, A4 and M3, we have,

$\frac{GW|\equiv\#(r_{GW})}{GW|\equiv\# r_{GW}, M \xleftrightarrow{k_S} GW}$ (Freshness rule)

$\frac{GW|\equiv M \xleftrightarrow{k_{GW}^{(M)}} GW, GW \triangleleft \{(r_{GW}, M \xleftrightarrow{k_S} GW)\}_{k_{GW}^{(M)}}}{GW|\equiv M|\sim(r_{GW}, M \xleftrightarrow{k_S} GW)}$ (Message meaning rule)

$\frac{GW|\equiv\#(r_{GW}, k_S), GW|\equiv M|\sim(r_{GW}, M \xleftrightarrow{k_S} GW)}{GW|\equiv M|\equiv r_{GW}, M \xleftrightarrow{k_S} GW}$ (Nonce verification rule)

$\frac{GW|\equiv M|\equiv(r_{GW}, M \xleftrightarrow{k_S} GW)}{GW|\equiv M|\equiv(M \xleftrightarrow{k_S} GW)}$ (Belief rule)

Thus, goal G2 is reached.

$\frac{GW|\equiv M|\equiv(r_{GW}, M \xleftrightarrow{k_S} GW)}{GW|\equiv M|\equiv r_{GW}}$ (Belief rule)

Thus, goal G3 is satisfied.

- From assumption A5 and A6 we have,

$\frac{GW|\equiv M\Rightarrow(M \xleftrightarrow{k_S^{(M)}} GW), GW|\equiv M|\equiv(M \xleftrightarrow{k_S} GW)}{GW|\equiv(M \xleftrightarrow{k_S} GW)}$ (Jursdiction rule)

Thus, goal G1 is reached.

Lemma 2: Assuming E used in protocol II is a secure pseudo- random function family, then protocol II utilizing E is a secure mutual entity authentication and key exchange protocol.

Proof:

Idealization:

- M1: $M \rightarrow S$:-
- M2, M3: $S \rightarrow M \rightarrow GW$:

$\{(S \xleftrightarrow{k_{GW}^{(S)}} GW, M \xleftrightarrow{k_{GW}^{(M)}} GW, r_S)\}_{k_{GW}^{(S)}}$

- M4: $GW \rightarrow M$:

$\{[r_M, k_M^{(S)}, S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M),$
$\{k_M^{(S)}, S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M), r_S)\}_{k_{GW}^{(S)}}]\}_{k_{GW}^{(M)}}$.

- M5: M $\rightarrow$S:

$\{(k_M^{(S)}, S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M), r_S)\}_{k_{GW}^{(S)}}$.

Assumptions. The assumptions of the protocol are as follows:

$$M| \equiv \#(r_M), S| \equiv \#(r_S), M| \equiv M \xleftrightarrow{k_{GW}^{(M)}} GW,$$
$$S| \equiv S \xleftrightarrow{k_{GW}^{(S)}} GW, GW| \equiv M \xleftrightarrow{k_{GW}^{(M)}} GW,$$
$$GW| \equiv S \xleftrightarrow{k_{GW}^{(S)}} GW, S|$$
$$\equiv GW \Rightarrow (S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M)),$$
$$M| \equiv GW \Rightarrow (S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M))$$

Main goals. The main goals of protocol II are,

- G1: $S| \equiv (S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M))$

G2: $M| \equiv (S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M))$

Analysis.

- From messages M2,M3 and the assumptions, we have,

$$GW| \equiv S \xleftrightarrow{k_{GW}^{(S)}} GW,$$
$$\frac{GW \triangleleft \{(M \xleftrightarrow{k_{GW}^{(M)}} GW, S \xleftrightarrow{k_{GW}^{(S)}} GW, r_s)\}_{k_{GW}^{(S)}}}{GW| \equiv S| \sim r_S}$$

(Message meaning rule)

- From message M5 and the assumptions, we have the following rules and the first jurisdiction rule, as shown at the top of the next page:

$$\frac{S|\equiv S \xleftrightarrow{k_{GW}^{(S)}} GW, S \triangleleft \{(k_M^{(S)}, S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M), r_s)\}_{k_{GW}^{(S)}}}{S|\equiv GW|\sim(k_M^{(S)}, S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M), r_S)}$$

(message meaning rule)

$\frac{S|\equiv\#(r_S)}{S|\equiv\#(k_M^{(S)}, S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M), r_s)}$ (freshness rule)

$$\frac{S|\equiv\#(k_{GW}^{(S)}), S \xleftrightarrow{k_M^{(S)}} M, r_s), S|\equiv GW|\sim(k_M^{(S)}, S \xleftrightarrow{k_M^{(S)}} M, r_s)}{S| \equiv GW|\equiv(k_M^{(S)}, S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M, r_s)}$$

(nonce verification rule)

This satisfies goal G1.

- From M4 and the assumptions, we have the following rules and the second jurisdiction rule, as shown at the top of the next page:

$$\frac{M|\equiv M \xleftrightarrow{k_{GW}^{(M)}} GW, M \triangleleft \{[r_M, k_M^{(S)}, S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M), \{(k_M^{(S)}, S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M), r_s)\}_{k_{GW}^{(S)}}]\}_{k_{GW}^{(M)}}}{M| \equiv GW| \sim (r_M, k_M^{(S)}, S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M), \{(k_M^{(S)}, S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M), r_s)\}_{k_{GW}^{(S)}})}$$

(Message meaning rule)

$$\frac{M| \equiv \#(r_M)}{M| \equiv \#(r_M, k_M^{(S)}, S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M), \{(k_M^{(S)}, S \xleftrightarrow{k_M^{(S)}} M \#(S \xleftrightarrow{k_M^{(S)}} M), r_s)\}_{k_{GW}^{(S)}})}$$

(Freshness rule)

$\frac{M|\equiv\#(X), M|\equiv GW|\sim X}{M|\equiv GW|\equiv X}$ (nonce verification rule),where

This satisfies goal G2.One may verify that the two secondary goals:

$S| \equiv M| \equiv (S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M)$ and $M| \equiv S| \equiv (S \xleftrightarrow{k_M^{(S)}} M, \#(S \xleftrightarrow{k_M^{(S)}} M))$ are also satisfied.

$$\frac{S|\equiv GW \Rightarrow (S \overset{k_M^{(S)}}{\longleftrightarrow} M, \#(S \overset{k_M^{(S)}}{\longleftrightarrow} M), S|\equiv GW|\equiv (S \overset{k_M^{(S)}}{\longleftrightarrow} M, \#(S \overset{k_M^{(S)}}{\longleftrightarrow} M)}{S|\equiv (S \overset{k_M^{(S)}}{\longleftrightarrow} M, \#(S \overset{k_M^{(S)}}{\longleftrightarrow} M)} \text{(Jurisdiction rule)}$$

$$X = r_M, k_M^{(S)}, S \overset{k_M^{(S)}}{\longleftrightarrow} M, \#(S \overset{k_M^{(S)}}{\longleftrightarrow} M), \{(k_M^{(S)}, S \overset{k_M^{(S)}}{\longleftrightarrow} M, \#S \overset{k_M^{(S)}}{\longleftrightarrow} M), r_s)\}_{k_{GW}^{(S)}}$$

$$\frac{M|\equiv GW \Rightarrow (S \overset{k_M^{(S)}}{\longleftrightarrow} M, \#(S \overset{k_M^{(S)}}{\longleftrightarrow} M), M|\equiv GW|\equiv (S \overset{k_M^{(S)}}{\longleftrightarrow} M, \#(S \overset{k_M^{(S)}}{\longleftrightarrow} M)}{M|\equiv (S \overset{k_M^{(S)}}{\longleftrightarrow} M, \#(S \overset{k_M^{(S)}}{\longleftrightarrow} M))} \text{(Jurisdiction rule)}$$

Lemma 3: Assuming E used in protocol III is a secure pseudo-random function family, then protocol III utilizing E is a secure mutual entity authentication and key exchange protocol.

Proof:

Idealization

- M1: $S_d \rightarrow S_c : -$
- M2:

$$S_c \rightarrow GW : \{(S_c \overset{k_{GW}^{(S_c)}}{\longleftrightarrow} GW, S_d \overset{k_{GW}^{(S_d)}}{\longleftrightarrow} GW, r_{S_c}, r_{S_d})\}_{k_{GW}^{(S_c)}}$$

- M3:

$$GW \rightarrow S_c : \{(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d, r_{s_d}, k_{S_c}^{(S_d)})\}_{k_{GW}^{(S_d)}},$$
$$\{(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d, r_{S_c}, k_{S_c}^{(S_d)}, S_c \overset{K}{\longleftrightarrow} GW)\}_{k_{GW}^{(S_c)}}$$

- M4:

$$S_c \rightarrow S_d : \{(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d, r_{s_d}, k_{S_c}^{(S_d)})\}_{k_{S_c}^{(S_d)}},$$
$$\{(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d, r_{s_d}, r_{s_c})\}_{k_{S_c}^{(S_d)}}$$

- M5: $S_d \rightarrow S_c : \{(r_{s_d})\}_{k_{S_c}^{(S_d)}}$

Assumptions.

$$S_c|\equiv \#(r_{s_c}),\ S_d \equiv \#(r_{S_d}),\ S_c|\equiv S_c \overset{k_{GW}^{(S_c)}}{\longleftrightarrow} GW,\ S_d| \equiv S_d \overset{k_{GW}^{(S_d)}}{\longleftrightarrow} GW,$$

$$GW|\equiv S_c \overset{k_{GW}^{(S_c)}}{\longleftrightarrow} GW, GW|\equiv S_d \overset{k_{GW}^{(S_d)}}{\longleftrightarrow} GW,$$

$$S_c|\equiv GW \Rightarrow (S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d, \#(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d)),$$

$$S_d|\equiv GW \Rightarrow (S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d, \#(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d)),$$

$$S_c|\equiv GW \Rightarrow (S_c \overset{K}{\longleftrightarrow} GW, \#(S_c \overset{K}{\longleftrightarrow} GW))$$

Main Goals. The main goals of protocol III

- **G1:** $S_c|\equiv (S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d, \#(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d))$
- **G2::** $S_d|\equiv (S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d, \#(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d))$
- **G3::** $S_c|\equiv (S_c \overset{K}{\longleftrightarrow} GW, \#(S_c \overset{K}{\longleftrightarrow} GW))$

Analysis.

- From M2 and the assumptions,

$$\frac{GW|\equiv (S_c \overset{k_{GW}^{(S_c)}}{\longleftrightarrow} GW,\ GW \triangleleft \{(S_c \overset{k_{GW}^{(S_c)}}{\longleftrightarrow} GW, S_d \overset{k_{GW}^{(S_d)}}{\longleftrightarrow} GW, r_{s_c}, r_{s_d})\}_{k_{GW}^{(S_c)}}}{GW|\equiv S_c| \sim (r_{s_c}, r_{s_d})}$$

(Message meaning rule)

- From message M3 and the assumptions,

$$\frac{S_c|\equiv S_c \overset{k_{GW}^{(S_c)}}{\longleftrightarrow} GW,\quad S_c \triangleleft \{(S_c \overset{k_{s_c}^{(S_d)}}{\longleftrightarrow} S_d, r_{s_c}, k_{S_c}^{(S_d)}, S_c \overset{K}{\longleftrightarrow} GW)\}_{k_{GW}^{(S_c)}}}{S_c|\equiv GW| \sim (S_c \overset{k_{s_c}^{(S_d)}}{\longleftrightarrow} S_d, r_{s_c}, k_{S_c}^{(S_d)}, S_c \overset{K}{\longleftrightarrow} GW)}$$

(Message meaning rule)

$$\frac{S_c|\equiv \#(r_{s_c})}{S_c|\equiv \#(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d, r_{s_c}, k_{S_c}^{(S_d)}, S_c \overset{K}{\longleftrightarrow} GW)}$$

(Freshness rule)

$$\frac{S_c|\equiv \#(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d, r_{S_c}, k_{S_c}^{(S_d)}, S_c \overset{K}{\longleftrightarrow} GW),\quad S_c|\equiv GW| \sim (S_c \overset{k_{s_c}^{(S_d)}}{\longleftrightarrow} S_d, r_{s_c}, k_{s_c}^{(S_d)}, S_c \overset{K}{\longleftrightarrow} GW)}{S_c|\equiv GW|\equiv (S_c \overset{k_{s_c}^{(S_d)}}{\longleftrightarrow} S_d, r_{s_c}, k_{s_c}^{(S_d)}, S_c \overset{K}{\longleftrightarrow} GW)}$$

(Nonce verification rule)

$$\frac{S_c|\equiv GW \Rightarrow S_c \overset{k_{s_c}^{(S_d)}}{\longleftrightarrow} S_d, \#(S_c \overset{k_{s_c}^{(S_d)}}{\longleftrightarrow} S_d),\quad S_c|\equiv GW \equiv (S_c \overset{k_{s_c}^{(S_d)}}{\longleftrightarrow} S_d, \#(S_c \overset{k_{s_c}^{(S_d)}}{\longleftrightarrow} S_d)}{S_c|\equiv (S_c \overset{k_{s_c}^{(S_d)}}{\longleftrightarrow} S_d, \#(S_c \overset{k_{s_c}^{(S_d)}}{\longleftrightarrow} S_d)}$$

(Jurisdictionrule)

This satisfies goal G1

$$\frac{S_c|\equiv GW \Rightarrow S_c \overset{K}{\longleftrightarrow} GW, \#(S_c \overset{K}{\longleftrightarrow} GW),\quad S_c|\equiv GW \equiv (S_c \overset{K}{\longleftrightarrow} GW, \#(S_c \overset{K}{\longleftrightarrow} GW)}{S_c|\equiv (S_c \overset{K}{\longleftrightarrow} GW, \#(S_c \overset{K}{\longleftrightarrow} GW)}$$

(Jurisdictionrule)

This satisfies goal G1

- From message M4 and the assumptions

$$\frac{S_d| \equiv S_d \overset{k_{GW}^{(S_d)}}{\longleftrightarrow} GW,\ S_d \lhd \{(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d,\ r_{S_d},\ k_{S_c}^{(S_d)})\}_{k_{GW}^{(S_d)}}}{S_c| \equiv GW \mid \sim (S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d,\ r_{S_d},\ k_{S_c}^{(S_d)})}$$

(Message meaning rule)

$$\frac{S_d| \equiv \#(r_{S_d})}{S_d| \equiv \#(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d, r_{S_d}, k_{S_c}^{(S_d)})}$$ (Freshness rule)

$$\frac{S_d| \equiv \#(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d,\ r_{S_d},\ k_{S_c}^{(S_d)}),\quad S_d| \equiv GW \mid \sim (S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d,\ r_{S_d},\ k_{S_c}^{(S_d)})}{S_d| \equiv GW \mid \equiv (S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d,\ r_{S_c},\ k_{S_c}^{(S_d)})}$$

(Nonce verification rule)

$$\frac{S_d| \equiv GW \Rightarrow (S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d\ ,\ \#(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d),\quad S_d| \equiv GW \mid \equiv (S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d,\ \#(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d)}{S_d| \equiv (S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d, \#(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d)}$$

(Jurisdiction rule)

This satisfies goal G2.

The second encryption of M4 and encryption in message M5 satisfy the secondary goals:

$$S_c| \equiv S_d| \equiv (S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d\ \#(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d))$$

and

$$S_d| \equiv S_c| \equiv (S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d\ \#(S_c \overset{k_{S_c}^{(S_d)}}{\longleftrightarrow} S_d)).$$

The proof for protocol IV follows in a similar way to the proof of protocol II and III and hence, omitted. We now state the following theorem:

Theorem 1: The M2M authentication scheme presented in this paper is a secure M2M mutual authentication and key exchange scheme assuming H and E are secure pseudo-random functions.

Proof: The proof follows from ***Lemma*1**, ***Lemma*2** and ***Lemma*3**.

VI. EFFICIENCY EVALUATION

This section is about the evaluation of the efficiency of the proposed scheme.

A. STORAGE REQUIREMENTS

M2M Service Provider *(MSP)*: The MSP is required to store her own master key k_{MSP}, her signature key sk_{MSP} and the public keys of all gateways under her authority. It is required to store the identity of each registered mobile device ID_M as well as his secret key k_M.

M2M Gateway *(GW)*: Each GW is required to store the signature verification key pk_{MSP} of MSP, its own private key sk_{GW}, the tuple $(ID_M, k_{GM}^{(M)})$ for each mobile user M and the tuple $(ID_S, k_{GM}^{(S)})$ for each sensor S in the domain.

TABLE 2. Computation cost of the proposed scheme.

Entity	Protocol I	Protocol II	Protocol III	Protocol IV	Total
Gateway	$2c_{sym} = 2c_h$	$3c_{sym} = 3c_h$	$3c_{sym} = 3c_h$	$3c_{sym} = 3c_h$	$11c_h$
Mobile user	$1c_h + 2c_{sym} = 3c_h$	$2c_{sym} = 2c_h$	-----	-----	$5c_h$
Sensor	---	$2c_{sym} = 2c_h$	$3c_{sym} = 3c_h$	$6c_{sym} = 6c_h$	$11c_h$

Mobile user *M*: Is required to store the tuple (ID_M, k_M) in addition to the identities of the sensors he communicates with.

Sensor node *S*: Each sensor node is required to store its shared key $k_{GM}^{(S)}$ with the GW.This is in addition to the identities of other sensors in its area.

B. COMPUTATION COMPLEXITY

The computation cost is described next.

Mobile user *M*: In protocol I, M performs a hash invocation, a symmetric encryption and a symmetric decryption. In protocol II, M performs a symmetric encryption and a symmetric decryption using $k_{GM}^{(M)}$.

Sensor node *S*: In protocol II, S performs one invocation of symmetric encryption and one invocation of symmetric decryption. In protocol III, S_c performs two symmetric encryptions and one symmetric decryption. S_d performs one symmetric decryption and one symmetric encryption. We take the larger cost as the sensor cost for this protocol. Protocol IV requires double the cost of protocol III.

Gateway *GW*: In protocol I, GW is required to perform a symmetric encryption and a symmetric decryption. In protocol II, GW performs a symmetric decryption and two symmetric encryptions. The cost in protocol III is one symmetric key decryption and two symmetric encryptions. Protocol IV is the same as protocol III.

C. COMPUTATION COST

Let c_h be the computation time of one hash invocation. One symmetric encryption costs roughly the same as a one hash invocation. Based on this assumption, Table 2 shows the computation time of each entity in each protocol with c_h as the time unit.

D. COMPUTATION TIME

Recalling the experimental results of [15] where the authors have implemented cryptographic primitives on different brands of smartcards and mobile phones manufacturers. An implementation of SHA-1 on Oberthur ID-one v7.0a smart card takes on the average of 50 ms, while it takes 0.02 ms on ASUS-TF300T tablet. Based on these results, the computation time of each protocol in the proposed scheme is given in Table 3.

TABLE 3. Computation time for *M* & *S* in the proposed scheme on mobile devices and smart cards.

Entity	Protocol I	Protocol II	Protocol III	Protocol IV	Total
ASUS-TF300T	M : 0:06 ms S : --	M : 0:04 ms S : 0:04 ms	M : -- S : 0:06 ms	M : -- S : 0:12 ms	M : 0:1 ms S : 0:22 ms
Oberthur ID-one v7.0-a	M : 150 ms S : --	M : 100 ms S : 100 ms	M : -- S : 150 ms	M : -- S : 300 ms	M : 250 ms S : 550 ms

TABLE 4. Computation cost of cryptographic operations with time as C_H.

Notation	Definition	Cost
c_h	Computation cost of one invocation of hash function	c_h
c_e	Computation cost of exponentiation in $G \times G$	$600c_h$
c_m	Computation cost of scalar multiplication in G	$72:5c_h$
c_p	Computation cost of pairing in $G \times G$	$1550c_h$
c_{sym}	Computation cost of symmetric encryption/decryption	c_h

TABLE 5. Comparison of computation costs with recent schemes.

Entity	Chen et al [1]	Sun et al [18]	The proposed scheme
MSP	$2c_e+3c_m+3c_p= 5857.5c_h$	$5c_h+2c_{sym} = 7c_h$	Not involved
Gateway	Not involved	Not involved	$11c_h$
Mobile user	$2c_e +4c_m+ 4c_p = 7690c_h$	$4c_h+c_{sym} = 5c_h$	$5c_h$
Sensor	$c_e+3c_m+ 3c_p = 5467.5c_h$	Not considered	$11c_h$
Total cost	**18525** c_h	**12** c_h	**27** c_h

VII. COMPARISONS

In this section, we compare the proposed scheme to other recently proposed schemes. However, other proposed schemes use different cryptographic operations. Therefore, we remind the experimental results attained in [16], [17], Table 4 displays the computation timings of various cryptographic operations mapped to the hash invocation time c_h as the time unit. We believe that this mapping to a unified time unit makes the comparison clearer.

Based on the information given in Table 4, we compare the computation cost of the proposed scheme with two recent schemes. We compare the proposed scheme with Chen et al. scheme [1] and Sun *et al.* scheme [18]. The comparison is given in Table 5.

As illustrated in Table 5, the proposed scheme proves extreme efficiency over the recent scheme of Chen *et al.* [1]. Their protocol requires a mobile user to perform computations that cost 7690 c_h while the sensor is required to perform a total of 5467.5 c_h. The proposed protocol requires the mobile user to perform computations equivalent to 5 c_h, while it requires 11 c_h for the sensor nodes.

In Sun *et al.* scheme [18], their protocol authenticates the mobile user to the *MSP*, but there is no consideration of authentication of the mobile user to the sensor nodes and how sensor nodes authenticate each other. In spite of these shortcomings, the efficiency of the proposed scheme is still closely comparable to their scheme. However, the proposed scheme provides a more complete service.

VIII. CONCLUSIONS

In the CPS, M2M is an emerging technology that promises to reduce the gap between the physical system and the cyber system. Authenticating machines in M2M networks is an important service that must exist to withstand different possible attacks against the M2M machines in M2M networks. We have proposed a scheme to realize this service. The proposed scheme allows any pair of entities in an M2M network to authenticate each other and establish a secure session key for exchanging private data. The proposed scheme eliminates the burden of the authentication process from the *MSP* and distributes this burden on the gateways under her authority. The mobile user, with only one master secret key provided by the *MSP* and roaming randomly in the M2M sites is able to authenticate with any of the gateways under the authority of this *MSP*. Using his master secret key, the mobile user is capable of authenticating any of the sensors in any M2M site. The proposed scheme allows any pair of sensors to authenticate each other with the help of this gateway. The authentication protocols in the proposed scheme do not rely on any public key cryptosystems.

The proposed scheme is quite low at computation and communication cost as it requires few invocations of hash functions and symmetric key encryptions/decryptions. As a result, the proposed scheme is lightweight and suitable for devices with very limited resources. We have proved the security of the proposed scheme using the BAN logic. We have showed the proposed scheme to withstand different potential adversarial attacks. We have evaluated the efficiency of the proposed scheme and compared it to recent protocols. From the entire study, we conclude that the proposed scheme is efficient and suitable for M2M networks with mobile users having low powered devices.

REFERENCES

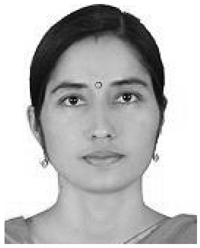
[1] S. Chen, M. Ma, and Z. Luo, "An authentication scheme with identity-based cryptography for M2M security in cyber-physical systems," *Secur. Commun. Netw.*, vol. 9, no. 10, pp. 1146–1157, 2016.

[2] W. Ren, L. Yu, L. Ma, and Y. Ren, "How to authenticate a device? Formal authentication models for M2M communications defending against ghost compromising attack," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 2, 2013, Art. no. 679450.

[3] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2008, pp. 495–500.

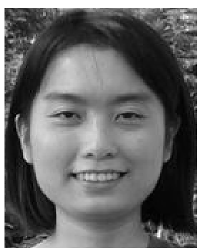
[4] Y. Zhang, W. Duan, and F. Wang, "Architecture and real-time characteristics analysis of the cyber-physical system," in *Proc. IEEE 3rd Int. Conf. Commun. Softw. Netw.*, May 2011, pp. 317–320.
[5] M. Chen, J. Wan, and F. Li, "Machine-to-machine communications: Architectures, standards and applications," *KSII Trans. Internet Inf. Syst.*, vol. 6, no. 2, pp. 480–497, 2012. doi: 10.3837/tiis.2012.02.002.
[6] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.
[7] M. Abadi and M. R. Tuttle, "A semantics for a logic of authentication," in *Proc. 10th Annu. ACM Symp. Princ. Distrib. Comput.*, 1991, pp. 201–216.
[8] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Comput. Elect. Eng.*, vol. 63, pp. 182–195, Oct. 2017.
[9] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 76, pp. 37–48, Dec. 2016.
[10] Q. Jiang, Y. Qian, J. Ma, X. Ma, Q. Cheng, and F. Wei, "User centric three-factor authentication protocol for cloud-assisted wearable devices," *Int. J. Commun. Syst.*, vol. 32, no. 6, 2019, Art. no. e3900. doi: 10.1002/dac.3900.
[11] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emerging machine to machine communications," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 28–35, Apr. 2011.
[12] S. Agarwal, C. Peylo, R. Borgaonkar, and J.-P. Seifert, "Operator-based over-the-air M2M wireless sensor network security," in *Proc. 14th Int. Conf. Intell. Next Gener. Netw. (ICIN)*, Oct. 2010, pp. 1–5.
[13] T.-D. Nguyen, A. Al-Saffar, and E.-N. Huh, "A dynamic id-based authentication scheme," in *Proc. 6th Int. Conf. Netw. Comput. Adv. Inf. Manage. (NCM)*, Aug. 2010, pp. 248–253.
[14] J.-M. Kim, H.-Y. Jeong, and B.-H. Hong, "A study of privacy problem solving using device and user authentication for M2M environments," *Secur. Commun. Netw.*, vol. 7, no. 10, pp. 1528–1535, 2014.
[15] J. Hajny, L. Malina, Z. Martinasek, and O. Tethal, "Performance evaluation of primitives for privacy-enhancing cryptography on current smart-cards and smart-phones," in *Data Privacy Management and Autonomous Spontaneous Security*. Springer, 2014, pp. 17–33.
[16] J.-J. Huang, W.-S. Juang, C.-I. Fan, and H.-T. Liaw, "Robust and privacy protection authentication in cloud computing," *Int. J. Innov. Comput., Inf. Control*, vol. 9, no. 11, pp. 4247–4261, 2013.
[17] X. Cao, W. Kou, and X. Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," *Inf. Sci.*, vol. 180, no. 15, pp. 2895–2903, 2010.
[18] X. Sun, S. Men, C. Zhao, and Z. Zhou, "A security authentication scheme in machine-to-machine home network service," *Secur. Commun. Netw.*, vol. 8, no. 16, pp. 2678–2686, 2015.

KM RENUKA received the M.Sc. degree from the Meerut College, Meerut, India, in 2003, and the M.Phil. degree in mathematics from Chaudhary Charan Singh University, Meerut, where she is currently pursuing the Ph.D. degree with the Department of Mathematics. She also qualified the National Eligibility Test conducted by CSIR, in 2005. She is actively engaged in analyzing and designing password-based authentication protocols.



SARU KUMARI received the Ph.D. degree in mathematics from Chaudhary Charan Singh University, Meerut, India, in 2012, where she is currently an Assistant Professor with the Department of Mathematics. She has published more than 133 research papers in reputed international journals and conferences, including 115 publications in SCI-indexed journals. Her current research interests include information security and applied cryptography. She is a Technical Program Committee Member for many international conferences. She is on the Editorial Board of more than 12 journals of international repute including seven SCI journals. She served as the Lead/Guest Editor of four Special Issues in SCI journals of Elsevier, Springer, and Wiley.

DONGNING ZHAO received the B.S. and M.S. degrees in communication engineering from the Nanjing Institute of Communication Engineering, Nanjing, China, in 2001 and 2004, respectively, and the Ph.D. degree in signal and information processing from Shenzhen University, in 2015. She is currently a Vice General Manager with Shenzhen Vetose Technology Co. Ltd., China. Her research interests include information security, information hiding, and multimedia processing.



LI LI received the B.S. degree in computer science and technology from the Harbin Institute of Technology, Weihai, China, in 2005, the M.E. degree in computer science and technology from the Harbin Institute of Technology, Shenzhen, China, in 2007, and the Ph.D. degree from the Harbin Institute of Technology (H.I.T), Shenzhen, in 2012. Her areas of interests are media security, image processing, the Internet of Things, and database security.