Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 679450, 9 pages
http://dx.doi.org/10.1155/2013/679450

Research Article

How to Authenticate a Device? Formal Authentication Models for M2M Communications Defending against Ghost Compromising Attack

Wei Ren,[1,2] Linchen Yu,[1] Liangli Ma,[3] and Yi Ren[4]

[1] *School of Computer Science, China University of Geosciences, Wuhan 430074, China*
[2] *Shandong Provincial Key Laboratory of Computer Network, Jinan 250014, China*
[3] *School of Electronic Engineering, Naval University of Engineering, Wuhan 430033, China*
[4] *Department of Computer Science, National Chiao Tung University, Hsinchu 30010, Taiwan*

Correspondence should be addressed to Wei Ren; weirencs@cug.edu.cn

Received 22 August 2012; Revised 27 November 2012; Accepted 29 November 2012

Academic Editor: Liguo Zhang

In Machine-to-Machine (M2M) communications, authentication of a device is of upmost importance for applications of Internet of Things. As traditional authentication schemes always assume the presence of a person, most authentication technologies cannot be applied in machine-centric M2M context. In this paper, we make the first attempt to formally model the authentication in M2M. We first model four attacking adversaries that can formulate all possible attacks in M2M, which are channel eavesdropping attack, credential compromise attack, function compromise attack, and ghost compromise attack. Next, we propose four models to tackle those corresponding adversaries, namely, credential-based model, machine-metrics-based model, reference-based model, and witness-based model. We also illustrate several concrete attacking methods and authentication approaches. We proof the authentication security for all proposed models and compare them for clarity. Our models present soundness and completeness in terms of authentication security, which can guide the design and analysis of concrete authentication protocols. Particularly, we construct a uniform authentication framework for M2M context and point out all possible authentication mechanisms in M2M.

1. Introduction

Machine-to-Machine (M2M) communication is a typical communication fashion in the Internet of Things (IoT). It has been envisioned as one of the most promising Internet-accessing approaches in the IoT for long-distance remote devices. M2M networking interface enables wide area communications for mobile or static devices, so that it is quit convenient and easy to deploy remote devices rapidly. M2M thus becomes a typical communication method for most IoT applications such as remote environmental sensing, long-distance controlling, moving object locating, and tracing. Besides, M2M communication further incorporates various novel applications such as smart grid [1], tele-medicine [2], and smart vehicles [3].

As remote devices are always located faraway in unattended or malicious environments, it is very likely that the devices may be hacked by attackers. For example, the software system in devices may be injected or infected by certain malicious codes, which may modify or fabricate forthcoming outgoing data. Moreover, the devices may perform arbitrary (Byzantine) misbehavior after being compromised. Thus, the data sent by remote sensing devices must be authenticated. Otherwise, remote receivers in the other end will receive a lot of garbage information and consequently respond falsely.

We note that the authentication in M2M context is quite different from traditional authentication. Roughly speaking, traditional authentication usually assume the entity being authenticated is a person, or human is involved in authentication procedures. Simply speaking, the authentication methods usually rely on three aspects: "what you know, what you have, and who you are." As the entity authentication in M2M is not a person, the traditional methods such as "what you know and who you are" may not be applied.

For example, password-based authentication (by manually inputting password) cannot be applied in M2M context. The biometric-based authentication such as fingerprint recognition cannot be applied in M2M context neither.

Furthermore, traditional authentication methods for wireless sensor networks (WSNs) may not be able to smoothly migrate to M2M situations. That is, the authentication methods in WSNs usually rely on certain secrete credentials in cryptographic building blocks, for example, secrete keys for symmetric key encryptions, or private keys for digital signatures. Those secrete credentials are stored in devices or chips attached to devices (e.g., smart cards). However, such an authentication method still cannot defend against all aforementioned attacks. For example, when devices are compromised, those credentials will be revealed by attackers, by hacking the devices or injecting malicious codes. It again shows the distinction between M2M authentication and person-based authentication where entities (i.e., persons) usually are assumed uncompromising.

Therefore, the entity authentication in M2M context must be reconsidered and reinspected. We also need to explore the tailored authentication methods in M2M context, to guarantee a stronger authentication (that will be formally defined later), in case the devices are compromised and credentials are exposed. Besides, the formal models for authentication are appealing, as the formal models can guarantee the security strength and clarify the core part out from various application details. Unfortunately, such problem has not been explored thoroughly until now, to the best of our knowledge.

Currently, although several related works start to concentrate on M2M security problems [4–8], the strong authentication methods in M2M have not been thoroughly explored yet [9–13]. In this paper, we make the first attempt to figure out the abstract models for M2M context. We adapt a formal and rigorous method used in modern or theoretic cryptography, to strictly state, present, and analyze the security of authentication. More specifically, we firstly formulate attack models regarding to device compromising in M2M context by using interactive Turing machine. We next categorize the classifications in M2M authentication and their security specification. Finally, we propose several abstract authentication models to address different attacking patterns and proof their security. All our presentations strictly follow the formal expressions for better clarity and rigorous generality.

The contributions of the paper are listed as follows: (1) we strictly formulate the possible attacks and adversaries in M2M, which facilities to clearly locate the security fragile point. For example, we point out credential compromising attack, function compromising attack, and ghost compromising attack; (2) we formulate the general and abstract authentication models with provable security in M2M context, which figures out the fundamental characteristics of all possible authentication methods in M2M to guide the further design and security analysis in practices; (3) we point out several concrete attacking methods and propose corresponding authentication approaches to illustrate our models.

The rest of the paper is organized as follows. In Section 2, we discuss the basic assumption and models used throughout the paper. Section 3 provides the detailed description of our proposed models and analysis. Section 4 gives an overview on relevant prior work. Finally, Section 5 concludes the paper.

2. Problem Formulation

2.1. Network Model. In most M2M communications, there exists two major entities: devices, denoted as Dev, and a central server.

Dev is defined to equip following components.

(1) Functional module, denoted as DevFM. It consists of software and hardware for generating sensing data, computing meta information, sending reports, receiving instructions, and acting accordingly. It usually has three folders in terms of functionality: (i) a communication module, usually enabling wide area communications (e.g., GRPS/CDMA/TD-LTE) to report data to a central server; (ii) a computing program processing the data; (iii) a storage system storing relevant code and the data.

(2) Credential module, denoted as DevCM. It consists of software and hardware for identification and credentials. One typical credential module is subscriber identification module (SIM) card, which stores unique identification and secretes credentials such as keys.

In this paper, we focus on above typical fashion in M2M communications—from devices to central servers. It is without loss of generality, because communications between devices and devices far away in M2M are usually relayed by a central server. As the devices are equipped with wide area communication capabilities, multihop M2M relay within remote devices rarely happen. The relay is usually unnecessary, as the devices can upload reports directly to central servers.

Even though multihop relay between devices happens, it is usually local area wireless communication such as wireless personal area network (WPAN), for example, Zigbee, or wireless local area network. That is, the reasonable architecture has two tiers: the communication between devices and gateways is WPAN, but the communication between gateways and a central server is M2M. In this case, the authentication of devices in the former tier has been explored in WSN communities and previous solutions can be migrated; the authentication of gateways in the latter tier is our focus. That is, in this scenario, we look on gateways as devices in our discussion.

In addition, no matter in which kind of authentication scenarios, we always assume the peer who authenticates (i.e., verifier) is trusted or secure. It is a baseline for the further meaningful discussion. We thus focus on the peer being authenticated (i.e., prover), which is a device in M2M scenarios. That is, how to authenticate a device in M2M.

2.2. Attack Model. It is required to consider the situation that devices may be compromised, as the devices may be always located in unattended environments. From the viewpoint of security strength, such assumption for the existence of stronger adversary will result in stronger security guarantee, which is mandatory for certain critical applications, such as

gas emission monitoring and back-bone smart grid. According to the modeling of networks and devices, we classify the attack models into four folders as follows.

(1) Channel eavesdropping attack, denoted as Attack_{ce}. It is a straightforward attack that adversaries sniff communication channels and try to subvert authentication methods, for example, revealing credentials.

(2) Credential Compromising Attack, denoted as Attack_{cc}. In this attack, the credential module is hacked, exposed, modified, cloned, or replaced by adversaries.

(3) Function compromising attack, denoted as Attack_{fc}. In this attack, the functional module is hacked, exposed, modified, cloned, or replaced by adversaries.

(4) Ghost compromising attack, denoted as Attack_{gc}. In this attack, the whole device can be hacked, exposed, modified, cloned, or replaced by adversaries. It can be looked as the combination of Attack_{cc} and Attack_{fc}.

Note that, the Attack_{cc} and Attack_{fc} may not be concurrent. For example, when tamper-proof hardware is applied for credential module, adversary's malicious code can only compromise function module, not credential module.

2.3. Security Definition. Roughly speaking, the secure authentication in this paper is defined as the interactive proof between two probabilistic polynomial interactive Turing machine (ITM) [14].

The ITM being authenticated is called Prover (denoted as $\mathscr{P}$); the ITM authenticating Prover is called Verifier (denoted as $\mathscr{V}$). The $\mathscr{P}$ and $\mathscr{V}$ both have one outgoing communication tape, one incoming communication tape, one input computing tape, one output computing tape, and one inner working tape. They also have other auxiliary tapes for interaction and security: one identity tape, one security parameter tape, one random tape, and one-bit activation tape. In this paper, the outgoing communication tape of $\mathscr{P}$ is the same with the incoming communication tape of $\mathscr{V}$. For simplicity, this tape is called interaction tape, denoted as $\mathscr{T}_i$.

The adversary (denoted as A) is also modeled as an ITM. In different attack models, adversaries have different corresponding capabilities. We list them from weaker one to stronger one incrementally. The stronger one inherently has the capability of the weaker one.

(1) In Attack_{ce}, the adversary is denoted as A_{ce}, which can read and write the interaction tape.

(2) In Attack_{cc} and not in Attack_{fc}, the adversary is denoted as A_{cc}, which can read and write the work tape. We assume it inherently has the capability of A_{ce}.

(3) In Attack_{fc} and not in Attack_{cc}, the adversary is denoted as $\mathscr{A}_{fc}$, which can also read and write input tape and output tape. We assume it inherently has the capability of A_{ce}.

(4) In Attack_{gc}, the adversary is denoted as $\mathscr{A}_{gc}$, which can also read and write all tapes.

As we have already stated, $\mathscr{V}$ needs to be secure (or honest) in authentication semantics.

Environmental ITM (denoted as $\mathscr{Z}$) exists. $\mathscr{Z}$ can read and write input tapes of $\mathscr{P}$ and $\mathscr{V}$. The protocol result is the output of $\mathscr{Z}$.

The one interaction between $\mathscr{P}$ and $\mathscr{V}$ can be modeled as follows.

(1) $\mathscr{P}$ writes outgoing communication tape $\mathscr{T}_i$;

(2) $\mathscr{V}$ reads incoming communication tape $\mathscr{T}_i$.

The sequence can be interchangeable. The times of interaction may be more than once.

Next, we state the definition of authentication and its security as follows:

Definition 1 (Authentication). From the transcripts on tape $\mathscr{T}_i$ by $\mathscr{V}$, $\mathscr{V}$ can believe the data is indeed from $\mathscr{P}$ (and data is not modified). More specifically, from tag in the transcripts {id, data, tag} on tape $\mathscr{T}_i$, $\mathscr{V}$ can believe data is indeed from the device $\mathscr{P}$ with the id without any change.

Definition 2. Security of Authentication of Protocol Π in the presence of adversary $\mathscr{A}$. From tag$'$ in {id, data$'$, tag$'$} in the protocol Π's transcripts that data are tampered to data$'$ by adversary $\mathscr{A}$, the probability that the adversary can fool $\mathscr{V}$ to believe data$'$ is from the device $\mathscr{P}$ with id without any change is negligible.

Define attack experiment $\mathsf{AuthFool}_{\mathscr{A},\Pi}(n)$ as follows:

(1) run protocol Π in the presence of adversary $\mathscr{A}$, where $\mathscr{P}$ and $\mathscr{V}$ are both ITM with security parameter n;

(2) $\mathscr{V}$ witnesses $\mathscr{A}$ tampered transcripts on tape $\mathscr{T}_i$ – {id, data$'$, tag$'$}, $\mathscr{V}$ output 1. That is, $\mathscr{V}$ believes that data$'$ come from the device $\mathscr{P}$ with id without any change. Otherwise, output 0;

(3) if and only if $\mathscr{V}$ output 1, the experiment output 1.

Definition 3. Authentication protocol Π is secure, if for any ITM adversary $\mathscr{A}$, it exists a negligible function negl satisfying

$$\Pr\left[\mathsf{AuthFool}_{\mathscr{A},\Pi}(n) = 1\right] \leq \mathsf{negl}(n). \tag{1}$$

Indeed, authentication can be further divided into two types: entity authentication and message authentication. Entity authentication is the concentration in this paper. Message authentication is however usually required also in communication context and can be attained with entity authentication together. We thus later do not explicitly split those two.

Definition 4 (Entity Authentication (Message Source Authentication)). From tag in the transcripts {id, data, tag} on tape $\mathscr{T}_i$, $\mathscr{V}$ can believe data is from the device $\mathscr{P}$ with id.

Definition 5 (Message Authentication (Message Integrity Authentication)). From tag in the transcripts {id, data, tag} on tape $\mathscr{T}_i$, $\mathscr{V}$ can believe data is transferred without any change.

Table 1: Notation.

$\mathscr{P}$	Prover
$\mathscr{V}$	Verifier
cred	Credential
id	Device identity
data	Reporting data
$\mathsf{negl}(n)$	Negligible function with parameter n

We can similarly define the attack experiment and corresponding security for entity authentication and message authentication.

3. Proposed Authentication Models

In this section, we propose a family of models to solve the authentication problem in M2M context.

We list all major notations used in the remainder of the paper in Table 1.

3.1. Defending Channel Eavesdropping Attack: Credential-Based Model (CBM). To defend Attack_{ce}, the simplest authentication model is credential-based model, where the authentication relies on the knowledge or possession of certain credentials, for example, secrete keys. The credential-based model is described as follows:

$$\begin{aligned} &\mathsf{MSG}_{\mathsf{cbm}} : \mathscr{P} \longrightarrow \mathscr{V} : \{\mathsf{id}, \mathsf{data}, \mathsf{tag} = f(\mathsf{cred} \| \mathsf{id} \| \mathsf{data})\}, \\ &\mathscr{V} : \mathrm{Verify}(\mathsf{id}, \mathsf{data}, \mathsf{tag}) \stackrel{?}{=} 1, \end{aligned} \tag{2}$$

where the Verify() is a tag verification function Verify(tag); $\mathsf{MSG}_{\mathsf{cbm}}$ is a message from $\mathscr{P}$ to $\mathscr{V}$; cred is a credential such as a secret key; $f()$ is a function with following properties.

(1) One-wayness. From $f(\mathsf{cred}\|\mathsf{id}\|\mathsf{data})$, it is computationally infeasible to compute cred, even if id, data and $f()$ are public. By using a formal notation, that is

$$\begin{aligned} &\left|\Pr\{\mathsf{cred} \mid f(\mathsf{cred} \| \mathsf{id} \| \mathsf{data}), \mathsf{id}, \mathsf{data}, f()\} - \Pr\{\mathsf{cred}\}\right| \\ &\quad \leq \mathsf{negl}(n), \end{aligned} \tag{3}$$

where $\mathsf{negl}(n)$ is a negligible function with parameter n. $\Pr\{A \mid B\}$ means given B the probability of event A (i.e., guessing right A). That is, any polynomial probabilistic Turing machine (PPTM) with parameter n cannot guess cred with noneligible probability, no matter whether $f(\mathsf{cred}\|\mathsf{id}\|\mathsf{data})$, id, data, $f()$ are given or not.

(2) Second-Preimage Resistance. Without cred, it is computationally infeasible to find another $\mathsf{id}'(\mathsf{id}' \neq \mathsf{id})$ such that $f(\mathsf{cred}\|\mathsf{id}'\|\mathsf{data}) = f(\mathsf{cred}\|\mathsf{id}\|\mathsf{data})$, even if data, id and $f()$ are public. Similarly, without cred, it is computationally infeasible to find another $\mathsf{data}'(\mathsf{data}' \neq \mathsf{data}$ satisfying $f(\mathsf{cred}\|\mathsf{id}\|\mathsf{data}) = f(\mathsf{cred}\|\mathsf{id}\|\mathsf{data}')$, even if data, id and $f()$ are public. That is,

$$\begin{aligned} &\Pr\left\{\mathsf{id}' \neq \mathsf{id}, f\left(\mathsf{cred} \left\| \mathsf{id}' \right\| \mathsf{data}\right)\right. \\ &\qquad \left. = f(\mathsf{cred} \| \mathsf{id} \| \mathsf{data}) \mid \mathsf{data}, \mathsf{id}, f()\right\} \leq \mathsf{negl}(n), \\ &\Pr\left\{\mathsf{data}' \neq \mathsf{data}, f\left(\mathsf{cred} \| \mathsf{id} \| \mathsf{data}'\right)\right. \\ &\qquad \left. = f(\mathsf{cred} \| \mathsf{id} \| \mathsf{data}) \mid \mathsf{data}, \mathsf{id}, f()\right\} \leq \mathsf{negl}(n). \end{aligned} \tag{4}$$

Certainly, $f(\mathsf{cred}\|\mathsf{id}\|\mathsf{data})$ can be easily computed if cred, id, and data are available, especially for resource constraint devices in M2M context. $f()$ can be instantiated with cryptographic primitives such as one-way function with second-preimage resistance, pseudorandom function, and trapdoor permutation.

Credential-based model can be further divided into two folders: one credential-based model and multicredential-based model. As it is named, multicredential-based model use multiple credentials in each $\mathsf{MSG}_{\mathsf{cbm}}$ message or distinct credential in multiple $\mathsf{MSG}_{\mathsf{cbm}}$ messages.

For only guaranteeing the entity authentication, $\mathsf{MSG}_{\mathsf{cbm}}$ can be changed to $\mathsf{MSG}'_{\mathsf{cbm}} : \mathscr{P} \rightarrow \mathscr{V} : \{\mathsf{id}, \mathsf{data}, \mathsf{tag} = f(\mathsf{cred}\|\mathsf{id})\}$;
Similarly, for only guaranteeing the message authentication, $\mathsf{MSG}_{\mathsf{cbm}}$ can be changed to $\mathsf{MSG}''_{\mathsf{cbm}} : \mathscr{P} \rightarrow \mathscr{V} : \{\mathsf{id}, \mathsf{data}, \mathsf{tag} = f(\mathsf{cred}\|\mathsf{data})\}$.

Analysis

Definition 6 (Soundness). The designed protocol can guarantee the required security. That is, the designed protocol is the sufficient condition of the required security.

Definition 7 (Completeness). The required security needs the designed protocol to guarantee. That is, the designed protocol is the necessary condition of the required security.

Proposition 8. *Credential-based model* Π_{cbm} *is secure in* Attack_{ce}. *That is,*

$$\Pr\left[\mathsf{AuthFool}_{\mathscr{A}_{ce}, \Pi_{cbm}}(n) = 1\right] \leq \mathsf{negl}(n). \tag{5}$$

Proof. It can be proofed by similar methods in Universally Composable security [14]; hereby only sketch is given. The security of the proposed model is guaranteed by the security of $f()$. The rationale is from the Turing Test. There exist a reality model and an ideal model. From the viewpoint of environmental machine, if the reality model and ideal model are indistinguishable, the reality model will reach the security of the ideal model. In reality model, there exist adversary, prover, and verifier running protocol; In ideal model, there exist ideal function that emulates the protocol, dummy prover and dummy verifier, and simulated adversary that emulates all possible interactions and attacks. Ideal function is always secure (it is regarded as an imaged trusted third party). If the ideal model and reality model are indistinguishable from the viewpoint of environmental machine, the security of protocol will be guaranteed.

In other words, if environmental machine can distinguish the reality model and the ideal model, a new adversary can be

created to subvert a certain security assumption by revoking the environmental machine as a subfunction. In the ideal function, $f()$ is perfectly secure. In the reality model, $f()$ is assumed to satisfy certain security requirements (e.g., one-wayness and preimage resistance). If the ideal model is indistinguishable with reality model by environmental machine, the adversary will subvert the assumption by consulting the environmental machine. Finally, the proposition proofs the soundness of credential-based model. □

Proposition 9. *Credential-based model has completeness for defending Channel Eavesdropping Attack.*

Proof. The proof has two folders: the credential is required; the credential is presented properly. On the one hand, as devices need to distinguish themselves with others, they need to show their secretly possessed knowledge—credential—to proof their identity. Thus, there must exist a credential in the tuples in $\mathsf{MSG}_{\mathrm{cbm}}$ on the transcripts T_i. On the other hand, the credential must be secretly and properly presented, as the interaction tape T_i can be tampered by eavesdropping adversary $\mathscr{A}_{\mathrm{ce}}$. Thus, the presence of credential relies on $f()$ that has one-wayness and second-preimage resistance. □

Besides, multicredential-based model is securer than one credential-based model. That is, the exposure of one credential by eavesdropping adversary $\mathscr{A}_{\mathrm{ce}}$ will only result in subverting the authentication security guaranteed by that credential. If $\mathscr{P}$ has multiple credentials, the exposure of credentials will become more difficult. It is natural to extend the security discussion to following statement.

Definition 10 (Forward Authentication Security). That is, if current credential is exposed by eavesdropping adversary $\mathscr{A}_{\mathrm{ce}}$, the authentication security before exposure is still guaranteed.

Proposition 11. *In* Attack_{ce}*, multiple credentials that derive from one-way function can guarantee forward authentication security.*

Proof. By using one-way function f, $\mathrm{cred}_i = f(\mathrm{cred}_{i-1})$, $(1 \le i \le n)$, where $\mathrm{cred}_0 = \mathrm{cred}$. The sequence of using cred is from cred_n to cred_0. Due to the one-wayness of $f()$, it can guarantee the confidentiality of previous credentials, even if current used credential is revealed by $\mathscr{A}_{\mathrm{ce}}$. □

Proposition 12. *Credential-based model* Π_{cbm} *is not secure in* Attack_{ce}*. That is,*

$$\Pr\left[\mathsf{AuthFool}_{\mathscr{A}_{cc},\Pi_{cbm}}(n) = 1\right] > \mathsf{negl}(n). \tag{6}$$

Proof (Straightforward). The authentication security of credential-based model relies on the secrecy of credentials. The presence of $\mathscr{A}_{\mathrm{cc}}$ will reveal all credentials. Thus, the authentication security is broken. □

3.2. Defending Credential Compromising Attack: Machine-Metrics Based Model (MBM). If the attack model is strengthened to $\mathsf{Attack}_{\mathrm{cc}}$, the credential-based model will not be able to guarantee the security of authentication, as it is proofed in previous proposition.

For simple illustration of $\mathsf{Attack}_{\mathrm{cc}}$, we first point out an attack method called relocation attack.

Definition 13 (Credential Relocation Attack). It is an attack that the credentials are relocated to anther device. Although the received {id‖data‖tag} is verified valid at $\mathscr{V}$, the data do not come from the device with claimed id; indeed, the data come from another device with different id.

To tackle the $\mathsf{Attack}_{\mathrm{cc}}$, we propose a machine-metric based model (MBM). In this MBM model, the physical characteristics of devices are collected as the identification of devices. Suppose the physical characteristic space is S, which consists of n characteristics. That is, $S = \{\mathrm{char}_1, \mathrm{char}_2, \ldots, \mathrm{char}_n\}$. Software program $\mathrm{prgm}_i()$ returns $\mathrm{char}_i \in S, (i = 1, \ldots, n)$. The machine-metrics based model is described as follows:

$$\mathsf{MSG}_{\mathrm{mbm}} : \mathscr{P} \longrightarrow \mathscr{V} : \left\{\mathrm{id}, \mathrm{data}, i, \mathrm{tag} = f\left(\mathrm{prgm}_i() \,\|\mathrm{id}\|\, \mathrm{data}\right)\right\},$$
$$\mathscr{V} : \mathrm{Verify}\left(\mathrm{id}, \mathrm{data}, \mathrm{tag}\right) \stackrel{?}{=} 1, \tag{7}$$

where Verify() is a tag verification function (we assume $\mathscr{V}$ securely possesses a table $\mathrm{Tbl} = \langle i, \mathrm{char}_i\rangle$, $(i = 1, \ldots, n)$, and fetches char_i according to index i to verify received tag); $\mathsf{MSG}_{\mathrm{mbm}}$ is a message from device $\mathscr{P}$ to $\mathscr{V}$; $\mathrm{prgm}_i()$ is securely computed at functional module in $\mathscr{P}$ and it returns a characteristic char_i as a credential of $\mathscr{P}$; $f()$ is a function with one-wayness and second-preimage resistance; note that $f()$ can be securely computed by functional module.

If we look char_i as a credential in CBM model, we will have similar discussion as follows. $\mathrm{prgm}_i()$ and $f(\mathrm{prgm}_i()\|\mathrm{id}\|\mathrm{data})$, $(i = 1, \ldots, n)$ can be easily computed, especially for resource constraint devices in M2M context. $f()$ can be instantiated with cryptographic primitives such as one-way function with second-preimage resistance, pseudo-random function, and trapdoor permutation.

Machine-metrics based model can be further divided into two folders: one Machine-Metrics based model and multiple Machine-Metrics based model. As it is named, multiple Machine-Metrics based model use multiple $\mathrm{prgm}_i()$ in each $\mathsf{MSG}_{\mathrm{mbm}}$ message or distinct $\mathrm{prgm}_i()$ in multiple $\mathsf{MSG}_{\mathrm{mbm}}$ messages.

For only guaranteeing the entity authentication, $\mathsf{MSG}_{\mathrm{mbm}}$ can be changed to $\mathsf{MSG}'_{\mathrm{mbm}} : \mathscr{P} \to \mathscr{V} : \{\mathsf{id}, \mathsf{data}, i, \mathsf{tag} = f(\mathsf{prgm}_i()\|\mathsf{id})\}$; Similarly, for only guaranteeing the message authentication, $\mathsf{MSG}_{\mathrm{mbm}}$ can be changed to $\mathsf{MSG}''_{\mathrm{mbm}} : \mathscr{P} \to \mathscr{V} : \{\mathsf{id}, \mathsf{data}, i, \mathsf{tag} = f(\mathsf{prgm}_i()\|\mathsf{data})\}$.

Analysis

Proposition 14. *Machine-Metrics based model* Π_{mbm} *is secure in* Attack_{cc}*. That is,* $\Pr[\mathsf{AuthFool}_{\mathscr{A}_{cc},\Pi_{mbm}}(n) = 1] \le \mathsf{negl}(n)$.

Proof. As the function module is secure, adversary cannot compute $\mathrm{prgm}_i()$, $(i = 1, \ldots, n)$. It can be looked as a computed credential to guarantee the authentication security.

The proof thus is reduced to the proof of the Proposition 8. It proofs the soundness of Machine-Metrics based model. □

Proposition 15. *Machine-Metrics based Model has completeness for defending Credential Compromising Attack.*

Proof. The proof can be reduced to the proof of Proposition 9. Concretely, the proof has two folders: a new credential is required; the new credential is presented properly. On the one hand, as devices need to distinguish themselves with others, they need to show their secretly possessed knowledge—credential—to proof their identity. As the credential module can be compromised, the credential must come from the functional module. Thus, there must exist a credential in the tuples in $\mathsf{MSG}_{\mathrm{mbm}}$ on the transcripts T_i. On the other hand, the credential must be secretly and properly presented, as the interaction tape T_i can be tampered by eavesdropping adversary $\mathscr{A}_{\mathrm{ce}}$. Thus, the presentation of credential relies on f that has one-wayness and second-preimage resistance. Besides, if the credential is online computed (not stored) by functional module, the security will be enhanced, which is similar to the case of multiple credentials. □

Similarly, multiple Machine-Metrics based model is securer than one Machine-Metrics based model. The discussion is similar to the one in the previous section. In summary, Machine-Metrics based model can be looked as an analog of biometric-based authentication for human.

Proposition 16. *Machine-Metrics based model Π_{mbm} is not secure in Attack_{fc}. That is,*

$$\Pr\left[\mathsf{AuthFool}_{\mathscr{A}_{fc},\Pi_{mbm}}(n) = 1\right] > \mathsf{negl}(n). \tag{8}$$

Proof (Straightforward). The authentication security of Machine-Metrics based model relies on the secure computation of $\mathrm{prgm}_i()$, $(i = 1,\ldots,n)$. The presence of $\mathscr{A}_{\mathrm{fc}}$ will reveal all $\mathrm{prgm}_i()$, $(i = 1,\ldots,n)$. Thus, the authentication security is broken. □

We give three special illustrations on Machine-Metrics based model for defending $\mathsf{Attack}_{\mathrm{cc}}$ (e.g., Credential Relocation Attack).

Definition 17 (Computation-Based Authentication). Each time $\mathscr{V}$ sends a one-time random computational puzzle, $\mathscr{P}$ counts the computation duration time in microsecond or Central Process Unit (CPU) cycles as the result of $\mathrm{prgm}_i()$.

Example 18. $\mathscr{V}$ sends a computational puzzle $g^n \bmod p$, where p is a prime number; $2 < g < p$ is an integer; $n < p$ is a positive integer. $\mathscr{P}$ counts the computation duration time in microsecond as the computation characteristic, in other words, the returning result of $\mathrm{prgm}_i()$.

Definition 19 (Location-Based Authentication). $\mathscr{V}$ sends an one-time random location puzzle. $\mathscr{P}$ returns computed location values. $\mathscr{V}$ verifies the location characteristic of $\mathscr{P}$. That is, $\mathrm{prgm}_i()$ returns location values of $\mathscr{P}$.

Example 20. $\mathscr{V}$ sends an one-time random location puzzle: the distance from $\mathscr{P}$ to a randomly chosen point. $\mathscr{P}$ computes the distance value according to its location values such as global positions and latitudes, as the location characteristic, in other words, the returning result of $\mathrm{prgm}_i()$.

Similarly, we can further define authentication methods by requesting other physical characteristics such as memory size, hardware fingerprints. Note that such kind of requesting must be fresh and generated at real time.

3.3. Defending Function Compromising Attack: Reference-Based Model (RBM). If the attack model is strengthened to $\mathsf{Attack}_{\mathrm{fc}}$, the Machine-Metrics based model will not be able to guarantee the security of authentication, which is proofed in previous proposition.

To illustrate $\mathsf{Attack}_{\mathrm{fc}}$, we first point out two concrete attack methods called Characteristic Replication Attack and Data Pollution Attack.

Definition 21 (Characteristic Replication Attack). The set $S = \{\mathrm{char}_i,\ldots,\mathrm{char}_n\}$ is replicated to another device by attackers, and they will choose corresponding char_i by elements upon revoking of $\mathrm{prgm}_i()$.

Definition 22 (Data Pollution Attack). Data is polluted by attackers, although the credential is valid to make the data being authenticated. That is, $\mathscr{P} \rightarrow \mathscr{V} : \{\mathrm{id}, \mathrm{data}', \mathrm{tag} = f(\mathrm{cred}\|\mathrm{id}, \|\mathrm{data}')\}$, where data is changed to data' by adversary $\mathsf{Attack}_{\mathrm{fc}}$ after functional module is compromised.

To tackle the $\mathsf{Attack}_{\mathrm{fc}}$, we propose a reference-based model (RBM). In RBM model, the reference behavior of $\mathscr{P}$ (e.g., from previous data or other devices) will be checked for the trustworthiness of data.

The reference-based model is described as follows:

$$\begin{aligned}\mathsf{MSG}_{\mathrm{rbm}} &: \mathscr{P} \longrightarrow \mathscr{V} : \{\mathrm{id}, \mathrm{data}, \mathrm{tag} = f(\mathrm{cred}\,\|\mathrm{id}\|\,\mathrm{data})\},\\ \mathscr{V} &: \mathrm{Verify}() \stackrel{?}{=} 1,\end{aligned} \tag{9}$$

where the Verify() includes a tag verification function Verify(tag) and especially, an extra verification function for data, called Verify(data).

We give two special illustration on reference-based model in the following.

Definition 23 (History-Based Authentication). The authenticator $\mathscr{V}$ verifies the history behaviors (e.g., data) to authenticate the trustworthiness of current behavior of $\mathscr{P}$, for example, the trustworthiness of data. Concretely, the data filter method can be applied at $\mathscr{V}$, where data come from the history.

Example 24. Suppose the history set is S, which consists of n values. That is, $S = \{v_1, v_2, \ldots, v_n\}$. Suppose the history set is

trustworthy, the detection of abnormal data can be done by the following verification function:

$$\text{Verify}(\text{data}) = \text{iff}\left(\frac{(\text{data}-\overline{v})^2}{\sum_{i=1}^{n-1}(v_i-\overline{v})^2} < \text{th}, 1, 0\right), \quad (10)$$

where th is an alert threshold.

Definition 25 (Neighbor-Based Authentication). The authenticator $\mathscr{V}$ verifies the other $\mathscr{P}$'s behaviors (e.g., neighbors' reporting data) to authenticate the trustworthiness of current behavior of $\mathscr{P}$, for example, the trustworthiness of data. Concretely, the data filter method can be applied at $\mathscr{V}$, where the data come from neighbors.

Example 26. Similar to above example, suppose the neighbor set is S, which consists of n values. That is, $S = \{v_1, v_2, \ldots, v_n\}$. Suppose the neighbor set is trustworthy, the detection of abnormal data can be done by the following verification function:

$$\text{Verify}(\text{data}) = \text{iff}\left(\frac{(\text{data}-\overline{v})^2}{\sum_{i=1}^{n-1}(v_i-\overline{v})^2} < \text{th}, 1, 0\right), \quad (11)$$

where th is an alert threshold.

In the neighbor-based authentication, the reference set S may not be always trustworthy. That is, the values in S may come from other $\mathscr{P}$s that are untrustworthy. To deal with this issue, we propose extra two methods in the following.

Definition 27 (Trustworthy Stunt Authentication). The S is from other trustworthy $\mathscr{P}$s that are predeployed. That is, the authenticator $\mathscr{V}$ verifies the trusted stunt's report (e.g., data) to authenticate the trustworthiness of current behavior of $\mathscr{P}$, for example, the trustworthiness of data. The verification function in this situation is similar to history-based Authentication.

Definition 28 (Threshold Stunt Authentication). Suppose there exists at least α nodes in S that are trustworthy (i.e., not compromised) in neighbor-based authentication. Simply speaking, the verification function can be designed as follows: select the median $S - \alpha$ values in S and then use verification function similarly.

Analysis

Proposition 29. *Reference-based model* Π_{rbm} *is secure in* Attack_{fc}. *That is,*

$$\Pr\left[\mathsf{AuthFool}_{\mathscr{A}_{fc},\Pi_{rbm}}(n) = 1\right] \leq \mathsf{negl}(n). \quad (12)$$

Proof. The message source authentication is guaranteed by Proposition 8. The message integrity authentication is roughly guaranteed by history-based authentication and neighbor-based authentication in reference-based model. It proofs the soundness of reference-based model. □

Proposition 30. *Reference-based Model has completeness for defending Function Compromising Attack.*

Proof. As functional module can be compromised by $\mathscr{A}_{\text{gc}}$, computational credential (namely, $\text{prgm}_i()$ or char_i) may be revealed, which is so-called characteristic replication attack. Besides, even though credentials in credential module can grantee that data cannot be modified by adversaries in the channel, the data can still be modified at the devices after the functional module is compromised, which is so-called data pollution attack. Thus, credentials in credential module defend against the former one; history-based authentication and neighbor-based authentication defend against the latter one. □

Proposition 31. *Reference-based model* Π_{rbm} *is not secure in* Attack_{gc}. *That is,*

$$\Pr\left[\mathsf{AuthFool}_{\mathscr{A}_{gc},\Pi_{rbm}}(n) = 1\right] > \mathsf{negl}(n). \quad (13)$$

Proof (Straightforward). As the credential module can be compromised in $\mathscr{A}_{\text{gc}}$, the authentication security is broken. □

3.4. Defending Ghost Compromising Attack: Witness-Based Model (WBM). If the adversary has the most powerful strength, namely, the $\mathsf{Attack}_{\text{gc}}$. We point out it cannot be defended against by any authentication enhancement method only from $\mathscr{P}$.

Proposition 32. Attack_{gc} *cannot be defended only by* $\mathscr{P}$ *itself.*

Proof (Straightforward). As the credential module and functional module can both be compromised, any security enhancement will be also compromised. Thus, $\mathsf{Attack}_{\text{gc}}$ cannot be defended only by $\mathscr{P}$ itself merely. □

To tackle the $\mathsf{Attack}_{\text{gc}}$, we propose a witness-based model (WBM). In WBM model, environmental characteristics and device characteristics are both collected for the final authentication decision.

Suppose environmental characteristics consist of n components. That is, $S_e = \{\text{envr}_1, \text{envr}_2, \ldots, \text{envr}_n\}$. There exists at least one program $\text{wtns}_i()$ that can return $\text{envr}_i \in S_e$, $(i = 1, \ldots, n)$. In addition, suppose the device characteristics space is S_d, which consists of n characteristics. That is, $S_d = \{\text{char}_1, \text{char}_2, \ldots, \text{char}_n\}$. There exists at least one program $\text{prgm}_i()$ that can return $\text{char}_i \in S_d$, $(i = 1, \ldots, n)$. The witness-based model is described as follows:

$$\begin{aligned}\mathsf{MSG}_{\text{wbm}} : \mathscr{P} &\longrightarrow \mathscr{V} : \{\text{id}, \text{data}, \text{tag} \\ &= f\left(\text{cred} \parallel \text{prgm}_i() \parallel \text{id} \parallel \text{data}\right)\}, \\ \mathscr{V} &: \text{Verify}\left(\text{id}, \text{data}, \text{tag}\right) \stackrel{?}{=} 1,\end{aligned} \quad (14)$$

where the Verify() includes a tag verification function Verify(tag), a data verification function Verify(data), and an environment verification function Verify(envr).

Table 2: Comparison of attack models and authentication models.

Authentication model (Authentication illustration)	Attack model (Attack illustration)
Credential-based model	Channel eavesdropping attack
Machine-metrics-based model (Computation-based authentication) (Location-based authentication)	Credential compromising attack (Credential relocation attack)
Reference-based model (History-based authentication) (Neighbor-based authentication) (Trustworthy stunt authentication) (Threshold stunt authentication)	Function compromising attack (Characteristic replication attack) (Data pollution attack)
Witness-based model (Contamination-based authentication)	Ghost compromising attack

Table 3: Security comparison of models.

Authentication model	Authentication security
CBM	$\Pr[\mathsf{AuthFool}_{\mathscr{A}_{ce},\Pi_{cbm}}(n)=1] \le \mathsf{negl}(n)$ $\Pr[\mathsf{AuthFool}_{\mathscr{A}_{cc},\Pi_{cbm}}(n)=1] > \mathsf{negl}(n)$
MBM	$\Pr[\mathsf{AuthFool}_{\mathscr{A}_{cc},\Pi_{mbm}}(n)=1] \le \mathsf{negl}(n)$ $\Pr[\mathsf{AuthFool}_{\mathscr{A}_{fc},\Pi_{mbm}}(n)=1] > \mathsf{negl}(n)$
RBM	$\Pr[\mathsf{AuthFool}_{\mathscr{A}_{fc},\Pi_{rbm}}(n)=1] \le \mathsf{negl}(n)$ $\Pr[\mathsf{AuthFool}_{\mathscr{A}_{gc},\Pi_{rbm}}(n)=1] > \mathsf{negl}(n)$
WBM	$\Pr[\mathsf{AuthFool}_{\mathscr{A}_{gc},\Pi_{wbm}}(n)=1] \le \mathsf{negl}(n)$

We give an illustration for the witness-based authentication in the following.

Definition 33 (Contamination-Based Authentication). The authentication is provided by witness from other trustworthy peers in different channels.

Example 34. The authenticator $\mathscr{V}$ verifies whether $\mathscr{P}$ is touched or moved via the observation of protection lock or surveillance video camera. For example, $\mathrm{wtns}_1()$ returns lock status (suppose locked status is 1); $\mathrm{wtns}_2()$ returns whether camera picture is in static status (suppose static status is 1 means the monitored device is untouched). The Verify(envr) = $\mathrm{wtns}_1()$ .AND. $\mathrm{wtns}_2()$.

Analysis

Proposition 35. *Witness-based model* Π_{wbm} *is secure in* Attack_{gc}. *That is,*

$$\Pr\left[\mathsf{AuthFool}_{\mathscr{A}_{gc},\Pi_{wbm}}(n)=1\right] \le \mathsf{negl}(n). \quad (15)$$

Proof (Sketch). As the proof of authentication relies on the witness from others who are not compromised, the authentication security can be guaranteed. It proofs the soundness of witness-based model. □

Proposition 36. *Witness-based Model has completeness for defending Ghost Compromising Attack.*

Proof (Sketch). As the $\mathscr{P}$ can be totally compromised, the security enhancement for authentication must come from other trustworthy entities. □

Comparison. The security comparison of proposed models is compared and summarized in Tables 2 and 3.

4. Related Work

Security of M2M communications starts to attract more and more attentions [4, 5, 7, 8], but solutions for authentication in M2M context have not been thoroughly explored. Especially, the formal authentication models for M2M have been rarely discussed. In this paper, we made the first attempt in this regard. Zhang et al. [12] provided a practical group-based authentication for Machine Type Communication (MTC) scenario. Each device shares a secret key with home environment, and a group secret key with other devices in the same group. Their discussion focused on roaming cellular networks and human may be involved. He [10] proposed to use machine's fingerprint and encryption technique to conduct remote register authentication of software to prevent unauthorized use. It focused on software copyright safeguard. Lu et al. [5] first pointed out the reliability and security requirements in M2M communications. Many other works addressed security problems in smart grid scenarios, which may be related to M2M communications. For example, Fadlullah et al. [15] studied the detection of malicious activities in smart grid communication and proposed an early warning

system. Bartoli et al. [16] studied secure aggregation in smart grid M2M networks. They included the security design in the physical layer and MAC layer. Saied et al. [8] proposed a key establishment solution for heterogeneous M2M communications. Other works explored the security in a broader domain—IoT, which is relevant to M2M. For example, Alam et al. [17] studied the interoperability in security attributes between different administrative domains in IoT. They proposed a layered architecture of IoT framework. As the M2M is still undergoing development, several works studied M2M standards [6, 18–20]. For example, Bartoli et al. [6] reviewed the current undergoing standards for M2M communications.

5. Conclusions

In this paper, we made the first attempt to propose a family of formal models to authenticate devices in M2M context. We first modeled four attacking adversaries that can include all possible attacks in M2M. Next, we proposed four models to tackle corresponding adversaries. We also illustrated several concrete attacking methods and authentication approaches. We proofed the authentication security for all proposed models and compared them for clarity. Our models presented soundness and completeness with respect to necessary and sufficient conditions for authentication security, which can guide the design and analysis of concrete authentication protocols. Especially, we constructed a uniform authentication framework for possible various authentication approaches. Our model also pointed out all possible authentication mechanisms or sufficient solutions for authentications in M2M.

Acknowledgments

This research was financially supported by National Natural Science Foundation of China (no. 61170217), the Open Research Fund from Shandong provincial Key Laboratory of Computer Network (no. SDKLCN-2011-01), and Fundamental Research Funds for the Central Universities, China University of Geosciences (Wuhan) (nos. 110109 and 090109).

References

[1] J. Liu, X. Li, X. Chen, Y. Zhen, and L. Zeng, "Applications of internet of things on smart grid in China," in *Proceedings of the 13th International Conference on Advanced Communication Technology: Smart Service Innovation through Mobile Interactivity (ICACT '11)*, pp. 13–17, Seoul, South Korea, February 2011.

[2] X. M. Zhang and N. Zhang, "An open, secure and flexible platform based on internet of things and cloud computing for ambient aiding living and telemedicine," in *Proceedings of the International Conference on Computer and Management (CAMAN '11)*, pp. 1–4, Wuhan, China, May 2011.

[3] T. Tielert, M. Killat, H. Hartenstein, R. Luz, S. Hausberger, and T. Benz, "The impact of traffic-light-to-vehicle communication on fuel consumption and emissions," in *Proceedings of the 2nd International Internet of Things Conference (IoT '10)*, pp. 1–8, Tokyo, Japan, December 2010.

[4] I. Cha, Y. Shah, A. U. Schmidt, A. Leicher, and M. Meyerstein, "Addressing new security threats," *IEEE Vehicular Technology Magazine*, vol. 4, no. 3, pp. 69–75, 2009.

[5] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: the green, reliability, and security of emerging machine to machine communications," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 28–35, 2011.

[6] A. Bartoli, M. Dohler, J. Hernández-Serrano, A. Kountouris, and D. Barthel, "Low-power low-rate goes long-range: the case for secure and cooperative machine-to-machine communications," in *Proceedings of the IFIP TC 6th International Conference on Networking (Networking '11)*, vol. 6827 of *Lecture Notes in Computer Science*, pp. 219–230, Valencia, Spain, April 2011.

[7] D. A. Bailey, "Moving 2 mishap: M2M's impact on privacy and safety," *IEEE Security & Privacy*, vol. 10, no. 1, pp. 84–87, 2012.

[8] Y. B. Saied, A. Olivereau, and M. Laurent, "A distributed approach for secure M2M communications," in *Proceedings of the 5th International Conference on New Technologies, Mobility and Security (NTMS '12)*, pp. 1–7, Istanbul, Turkey, May 2012.

[9] X. Sun, S. Men, C. Zhao, and Z. Zhou, *A Security Authentication Scheme in Machine-to-Machine Home Network Service*, Security and Communication Networks, 2012.

[10] D. He, "Remote authentication of software based on machine's fingerprint," in *Proceedings of the IEEE 3rd International Conference on Software Engineering and Service Science (ICSESS '12)*, pp. 543–546, Beijing, China, June 2012.

[11] W. Zhang, Y. Zhang, J. Chen, Hui Li, and Y. Wang, "End-to-end security scheme for machine type communication based on generic authentication architecture," in *Proceedings of the 4th International Conference on Intelligent Networking and Collaborative Systems (INCoS '12)*, pp. 353–359, Bucharest, Romania, September 2012.

[12] Y. Zhang, J. Chen, H. Li, W. Zhang, J. Cao, and C. Lai, "Dynamic group based authentication protocol for machine type communications," in *Proceedings of the 4th International Conference on Intelligent Networking and Collaborative Systems (INCoS '12)*, pp. 334–341, Bucharest, Romania, September 2012.

[13] Z. Obrenović and B. den Haak, "Integrating user customization and authentication: the identity crisis," *IEEE Security & Privacy*, vol. 10, no. 5, pp. 82–85, 2012.

[14] R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols. Cryptology ePrint archive," Report 2000/067, 2000, http://eprint.iacr.org/ .

[15] Z. M. Fadlullah, M. M. Fouda, N. Kato, Xuemin Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," *IEEE Network*, vol. 25, no. 5, pp. 50–55, 2011.

[16] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure lossless aggregation over fading and shadowing channels for smart grid m2m networks," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 844–864, 2011.

[17] S. Alam, M. M. R. Chowdhury, and J. Noll, "Interoperability of security-enabled internet of things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 567–586, 2011.

[18] K. Chang, A. Soong, M. Tseng, and Z. Xiang, "Global wireless machine-to-machine standardization," *IEEE Internet Computing*, vol. 15, no. 2, pp. 64–69, 2011.

[19] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. D. Johnson, "M2M: from mobile to embedded internet," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 36–43, 2011.

[20] Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, and M. Guizani, "Home M2M networks: architectures, standards, and QoS improvement," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 44–52, 2011.