

Cyberentity Security in the Internet of Things

Huansheng Ning and Hong Liu, *Beihang University, China*

Laurence T. Yang, *Huazhong University of Science and Technology, China, and St. Francis Xavier University, Canada*

A proposed Internet of Things system architecture offers a solution to the broad array of challenges researchers face in terms of general system security, network security, and application security.

The Internet of Things (IoT) is emerging as an attractive future networking paradigm, in which each physical object is mapped as one or more cyberentities that can interact with other cyberentities, enabling pervasive connectivity. As cyberentities interact, they assume different characteristics in various across-space contexts.

The IoT poses a broad array of new challenges for researchers in terms of general system security,^{1,2} network security,³ and application security.⁴⁻⁶ There are three major obstacles to securing cyberentities in the IoT:

- *Expanding domains.* The mapping of physical objects in cyberspace, coupled with networking and communication cyberentities, make the scope of cyberentities in the IoT much larger than in the Internet.
- *Dynamic activity cycle.* Cyberentities might be simultaneously idle in some scenarios and active in others.
- *Heterogeneous interactions.* Interactions among cyberentities are not limited to cyber and physical

characteristics but also include social attributes, which are particularly important for across-space interactions.

To address these challenges, we propose a novel system architecture, the Unit and Ubiquitous IoT (U2IoT).⁷ A unit IoT is a single application, while the ubiquitous IoT includes interrelated local, national, and industrial IoTs.

SYSTEM ARCHITECTURE

As Figure 1 shows, the U2IoT has three layers: the *perception layer*, the *network layer*, and the *application layer*.

The perception layer includes technologies that sense physical objects and convert them into cyberentities. Major sensing technologies include radio-frequency identification (RFID), radar, infrared induction, the Global Positioning System (GPS), and Wi-Fi, Bluetooth, and ZigBee wireless sensor networks. This layer also includes mechanical and electronic actuators—valves and switches—that connect to the sensors and execute their instructions.

The network layer includes all network components—interfaces, routers, and gateways—and communication channels. *Management and data centers* act as network nodes; unit M&DCs are under the direct or indirect control of local (lM&DC), industrial (iM&DC), and national (nM&DC) entities. Heterogeneous network configurations can include the Internet, wireless sensor networks (personal area, local area, wide area, metropolitan area), and mobile and telecommunications networks. This layer

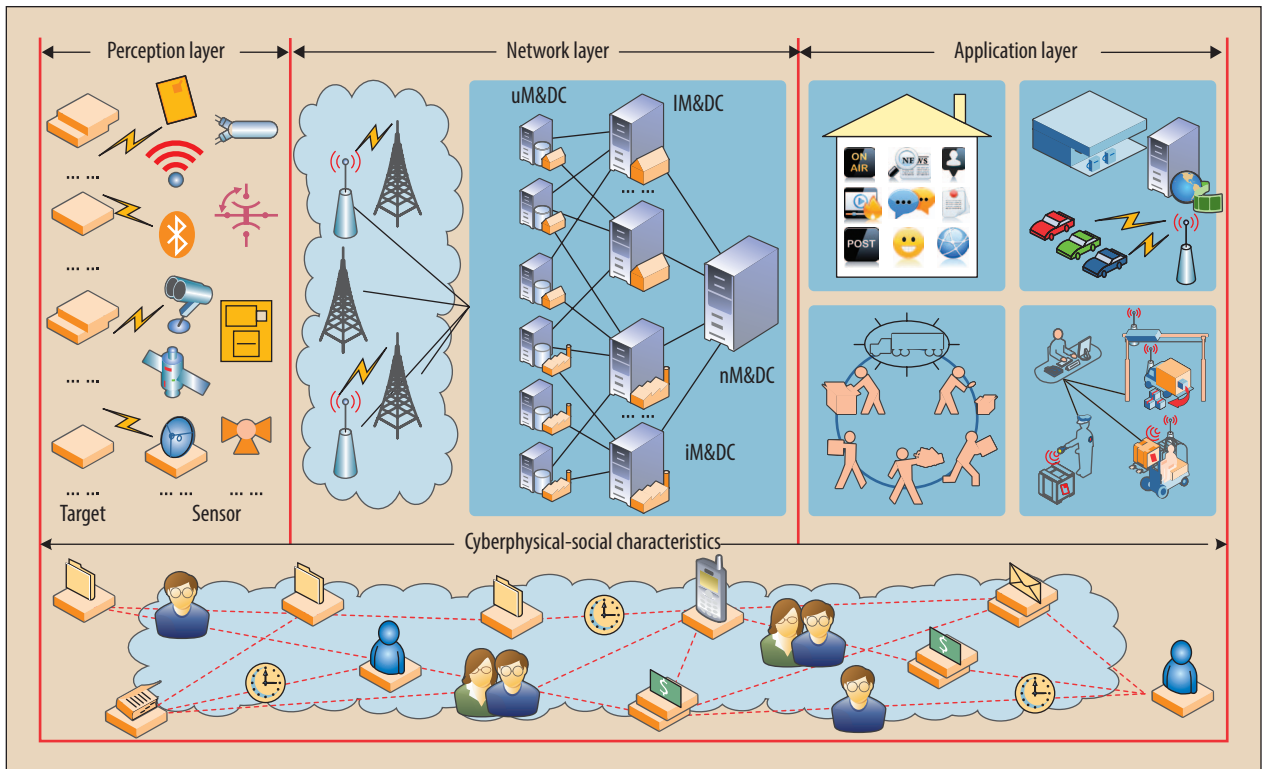


Figure 1. Unit and Ubiquitous IoT system architecture. The U2IoT has three layers: the perception layer, the network layer, and the application layer.

ensures reliable data transmission as well as connectivity by applying secure data coding, fusion, mining, and aggregation algorithms.

The application layer supports applications in local, industrial, and national IoTs managed respectively by IM&DCs, iM&DCs, and nM&DCs. A local IoT connects unit IoTs in a geographical region; an industrial IoT manages unit IoTs in an industry such as transportation or telecommunications; and a national IoT integrates a country's local and industrial IoTs. This layer also includes service integration, transnational supervision, and international coordination.

IoT applications ranging from smart homes to smart grids implement standard protocols such as the Constrained Application Protocol (CoAP) and Wireless Application Protocol (WAP), as well as widely accepted service-composition technologies such as service-oriented architectures and cloud computing.

Things in the U2IoT exist as both physical objects and cyberentities. The latter have four distinguishing characteristics.

Space-time consistency. A cyberentity can interact with other cyberentities at any time, at any place, and in any mode. Cyberentities can freely enter or leave such interactions without influencing ongoing sessions. To ensure space-time consistency, heterogeneous networks

incorporate registration, synchronization, and correlation policies and mechanisms.

Multi-identity coexistence. A cyberentity can have multiple identities, including a core identity and other temporary or assistant identities, according to its applications. These identities can be represented by various identifiers or nonidentifiers. For example, RFID-based inventory control systems assign tagged items a unique identifier such as an Electronic Product Code, while biometric measures such as fingerprints and iris scans serve as unique nonidentifiers. In other scenarios, nonunique identifiers and nonidentifiers can jointly represent things.

Dynamic interaction. A cyberentity can adapt to different environments and is directly or indirectly related to other cyberentities with which it interacts. Ubiquitous interactions across networks support intelligent data processing.

Social awareness. A cyberentity has social attributes that describe its relationships to physical objects. Such attributes include aspects such as ownership control management, affiliation relationship modeling, and behavior formalization.

CYBERENTITY DOMAINS

The U2IoT includes three main cyberentity domains: unit, ubiquitous, and logical.

Unit domain

The unit domain corresponds to unit IoT cyberentities including *cybertargets*, *cybersensors*, and *uM&DCs*. This domain is responsible for real-time target data collection, environmental monitoring, and basic information management.

Cybertargets consist of sensed data—for example, temperature, gas sensitivity, or blood pressure—of physi-

Cybersensors are either active or passive depending on whether they have a built-in power source.

cal, chemical, and biological parameters in surrounding environments as well as data attached to physical objects such as Quick Response codes.

Cybersensors are either active or passive depending on whether they have a built-in power source. Cybersensors such as radar, cameras, and thermocouples actively probe physical objects to acquire data about them, while cybersensors such as infrared sensors and resistance temperature detectors passively capture data projected from objects. Both types of cybersensors can apply the same sensing technology in different applications. For example, an active 2.4-GHz RFID tag has an on-board battery for identification in electronic toll collection, while backscattered signals trigger a passive 13.56-MHz RFID in supply chain management systems.

The *uM&DCs* act as intermediate network components between the unit and ubiquitous domains. They manage cybertarget and cybersensor interactions; perform storage, fusion, and mining on sensed data; and extract advanced knowledge to provide intelligent services, decision support, and real-time event response for unit IoTs.

Ubiquitous domain

The ubiquitous domain integrates multiple unit domains and constitutes the ubiquitous IoT's core. In this domain, cyberentities mainly include diverse *IM&DCs*, *iM&DCs*, and *nM&DCs* to manage local, industrial, and national IoTs, respectively.

Most *IM&DCs* use grid computing to manage loosely coupled and geographically dispersed local IoTs. Independent *IM&DCs* can also be organized in a cluster structure to collect data from local IoTs in different regions.

The *iM&DCs* use a hierarchical structure to manage industrial IoTs. They aggregate industrial IoTs with particular relationships and apply multiagent-based collaboration to manage layered data among different industries and industry chains.

The *nM&DCs* supervise local IoTs and industrial IoTs

within a country. They arbitrate disputes among local and industrial IoTs and interact with *iM&DCs* and *IM&DCs*, and with *nM&DCs* in other countries, to coordinate IoT services.

Logical domain

The logical domain defines relationships among cyberentities, which can be independent, affiliated, or inclusive/exclusive.

Independent. Some cyberentities do not depend on other cyberentities. In a smart home, for example, ambient brightness and gas density are independent cybertargets. Accordingly, a light-sensitive sensor and gas detector have distinct monitoring functions.

Affiliated. Many cyberentities are affiliated with other cyberentities either through *attribution* or *inheritance*. In the former case, cyberentities share attributes—for example, a smart home monitoring center is under the jurisdiction of its default community monitoring center. Alternatively, a cyberentity can inherit another cyberentity's attributes as well as have its own distinctive attributes. In a smart grid, for example, a power-line sensor and a smart meter have common sensing functions for data collection and transmission but also have unique characteristics dictated by their particular environments.

Inclusive/exclusive. Cyberentities can have overlapping or nonoverlapping relationships described by logical operators such as AND, OR, and NOT. A supply chain, for example, has multiple participants such as manufacturer, carrier, and retailer, with some cyberentities accessible to only one party and others accessible to multiple parties.

CYBERSECURITY REQUIREMENTS

The U2IoT has enhanced cybersecurity requirements with respect to the *CIA triad*, *authority*, *nonrepudiation*, and *privacy preservation*.

The *CIA triad* refers to the basic information security requirements of data confidentiality, integrity, and availability. Physical objects must be securely linked to their corresponding cyberentities and cyber-physical-social attributes.

Authority mainly refers to authentication and authorization. Single sign-on can be applied to achieve multiaccess authority, by which a single party can access a cyberentity without repetitive verification. Likewise, identification and verification procedures must be established to authorize access to heterogeneous networks.

Nonrepudiation provides proofs of a cyberentity's behaviors to a trusted third party.

Privacy preservation aims to protect sensitive information. Transparency is required to clarify which cyberentity owns which data and how that data is being used, while traceability is needed to identify a cyberentity's network connections.

Table 1. U2IoT attacks and countermeasures.

Attack category	Types of attacks	Possible consequences	Countermeasures
Gathering	Skimming: quickly reading transmitted messages to collect data	Loss of data confidentiality	Encryption and steganography
	Tampering: deliberately destroying or corrupting data	Loss of data integrity	Hash functions, cyclic redundancy checks, and message authentication codes
	Eavesdropping: collecting exchanged messages	Loss of data confidentiality	Encryption, identity-based authentication, and concealed data aggregation (CDA)
	Traffic analysis: monitoring exchanged data to determine traffic patterns	Loss of data confidentiality	Network forensics and misbehavior detection
Imitation	Spoofing: impersonating a user or program to obtain unauthorized access	Loss of data confidentiality and integrity	Identity-based authentication, key distribution, Internet Protocol Security, and digital signatures
	Cloning: duplicating and rewriting valid data into an equivalent entity	Loss of data confidentiality	Physically unclonable functions
	Replay: recording and storing previously transmitted data to repeat data or delay the current session	Loss of data confidentiality	Time stamps, time synchronization, pseudorandom numbers, session identifiers, and serial numbers
Blocking	Denial of service: Flooding data streams to deplete system resources or interfere with communications	Loss of data availability	Firewalls, router control, resource multiplication, distributed packet filtering, dynamic en-route filtering, and aggregate congestion control
	Jamming: electromagnetic interference or interdiction using the same frequency-band wireless signals	Loss of data availability	Antijamming, active jamming, and Faraday cages
	Malware: Distributing viruses, worms, Trojan horses, spyware, malicious adware, and other programs to interfere with systems	Loss of data confidentiality and availability	Antivirus programs, firewalls, and intrusion detection
Privacy	Individual: Deriving a user's locations, preferences, behaviors, and other private information	Loss of data confidentiality	Aggregated proofs, anonymous data transmission, CDA, and advanced digital signatures—for example, blind, group, and ring signatures
	Group: Deducing an organization's commercial interests and espionage	Loss of data confidentiality	Selective disclosure, data distortion, and data equivocation

THREATS AND VULNERABILITIES

In the U2IoT, attacks can be classified into four categories. *Gathering attacks* involve skimming or tampering with data, eavesdropping, and traffic analysis. *Imitation attacks* such as spoofing, cloning, and replay involve impersonation to obtain unauthorized access. *Blocking attacks* deplete system resources or interfere with communications using tactics such as denial of service (DoS), jamming, and malware. *Privacy attacks* seek to disclose sensitive information about individuals or groups. Attacks can occur independently or in concert, resulting in the loss of data confidentiality, integrity, and availability. Table 1 summarizes these threats and countermeasures.

The U2IoT also has several vulnerabilities related to

cybertargets, cybersensors, M&DCs, and networks that attackers can exploit.

Cybertargets. Dynamicity and mobility bring new challenges for cybertarget identification, in which the major threats are data interception and identity forgery. In vehicle-to-grid networks, for example, attackers can illegally capture a tagged vehicle battery's data and delete it, replace it, or insert new data to cheat a power aggregator.

Cybersensors. Because cybersensors are mainly resource-constrained devices with limited energy and storage, adversaries can actively intercept or manipulate data, or passively monitor data transmission. In ZigBee wireless sensor networks, for example, sensor and sink nodes are dynamically self-organized in a multihop manner, and

malicious nodes can be embedded in the area to communicate with neighbor nodes for data collusion.

M&DCs. Management and data centers confront similar threats to the Internet, such as DoS and distributed DoS attacks. In addition, emerging data management paradigms such as cloud storage and big data could compromise privacy. For example, data sharing supports intelligent decision making but puts data confidentiality at risk.

Various mandatory, discretionary, role-based, or attribute-based mechanisms can be used to control cyberentities' access to system resources.

Networks. Cybertargets and cybersensors primarily communicate through wireless channels, and such open interfaces have inherent defects. Bluetooth networks, for example, transmit mobile phones' multimedia data via peer-to-peer protocols that apply frequency-hopping spread spectrum modulation for data protection, which is vulnerable to eavesdropping. M&DCs mainly communicate with one another using mobile and telecommunications networks and the Internet. Next-generation technologies such as LTE-Advanced, WirelessMAN-Advanced, and IPv6 are still in their infancy, and robust mechanisms are needed to ensure reliable communications.

CYBERENTITY INTERACTION PHASES

Cyberentity interaction occurs in three phases. The *pre-active* phase is the state prior to launching a session such as accessing a network or a service, the *active* phase is the launched session, and the *postactive* phase is the state after the launched session. A comprehensive security solution addresses each of these phases.

Preactive phase security

Preactive phase security involves both symmetric and asymmetric key agreements for two or more cyberentities. Key distribution techniques include identity-based cryptography, schemes based on the bilinear Diffie-Hellman problem, and Tate pairing. Multiple cyberentities can adopt a group agreement to establish dynamic keys, with shortest-path tree-routing and multipath key reinforcement suitable for heterogeneous and cross-layer communications. Quantum cryptography uses Greenberger-Horne-Zeilinger states for key distribution to multiple entities.

Active phase security

Active phase security includes authentication, access control, secure routing, advanced signature algorithms, zero-knowledge proofs, and data aggregation.

Authentication. While validating interactive cyberentities traditionally relies on preshared secrets and trusted third parties, authentication should also consider network features such as heterogeneity, mobility, and scalability. Resource-constrained devices can apply ultralightweight algorithms such as bitwise operators, permutation, and pseudorandom numbers.

Other authentication options include lightweight algorithms such as hash functions, cyclic redundancy checks, and message authentication codes; full-fledged encryption/signature algorithms; and physical unclonable functions. In addition, the Internet Engineering Task Force has standardized the IP-based Protocol for carrying Authentication for Network Access (PANA), and multicast message and batch authentication are efficient for validating interactions among multiple cyberentities.

Access control. Various mandatory, discretionary, role-based, or attribute-based mechanisms can be used to control cyberentities' access to system resources. A semantic-based scheme is needed for Web services networks, while a trust-oriented approach is appropriate for the virtualization of cyberentities' social attributes. Conditional proxy re-encryption can be used to address data sharing and hiding in cloud computing environments.

Secure routing. Traditionally applied along with Internet Protocol Security, secure routing is becoming critical for mobile ad hoc networks. Heterogeneous sensing networks can incorporate multipath and on-demand routing protocols with tree-based, identity-based, and trust-based schemes to ensure secure data transmission.

Advanced signature algorithms. Blind, group, ring, identity, and other advanced signature algorithms can provide active phase security. Proxy and partially blind signatures can use bilinear maps for verification, while techniques such as elliptic curve cryptography can generate signatures. Certificateless signatures offer advantages in computational cost, and knowledge-based offline signatures can ensure forwarding security.

Zero-knowledge proofs. Used for identity verification between a prover and a verifier without revealing any sensitive information, zero-knowledge proofs include both an interactive and noninteractive mode. Different Σ -protocol composition modes including parallel, EQ, OR, and AND can be applied for aggregated proof verification. The blind watermark technique is suitable for zero-knowledge-based verification in lightweight applications.

Data aggregation. Algebraic or statistical computations aggregate sensed data prior to transmission. Concealed data aggregation can provide privacy homomorphism encryption to enhance security. Yoking or grouping proofs can aggregate sensed data for authentication. Homomorphic encryption and signature algorithms can perform hierarchical data aggregation to achieve data confidentiality and integrity in intranetworks and internetworks.

Postactive phase security

Postactive phase security includes intrusion detection, intrusion tolerance, and threshold cryptography.

Intrusion detection. Identifying malicious attacks in heterogeneous networks requires applying adaptive network intrusion detection algorithms. Artificial immune and neural networks can assist in identification and real-time monitoring, and data mining techniques such as feature selection and modeling can help locate infected nodes.

Intrusion tolerance and threshold cryptography. These techniques enable multiple cyberentities to collectively participate in secret management, with a share of the secret allocated to each entity. Even if a cyberentity is temporarily inactive or perennially unavailable, other legal cyberentities can perform normal interactions.

Other cryptographic algorithms can provide additional protection. For example, a dynamic group key agreement can apply threshold secret sharing to achieve key distribution among multiple cyberentities; segmentation can be introduced for distributed memory sharing; and a multi-level, compartmented, or multipartite hierarchical secret sharing scheme can be adapted to a hybrid network structure. Fragmentation redundancy scattering can enhance tolerance resilience, and IoT applications can apply dependable or hierarchical intrusion tolerance.

SECURING CYBERENTITY INTERACTION

Figure 2 shows three RFID-based interaction scenarios among U2IoT cyberentities. T refers to a tag (cybertarget), R indicates a reader (cybersensor), and IM&DC, iM&DC, and nM&DC connote unit, local, industrial, and national M&DCs, respectively; uM&DCI and uM&DCi signify uM&DCs with their corresponding default local and industrial M&DCs. Figure 3 shows proposed secure solutions for each scenario.

Scenario 1: Secure data access

In this scenario, T and R establish mutual authentication, and uM&DCI ensures that both are legal cyberentities. T and R are within the coverage of uM&DCI, which as a trusted entity can access the sensed tag data for management.

First, R generates an access challenge to T, which sends an authentication operator to R for verification. If T is

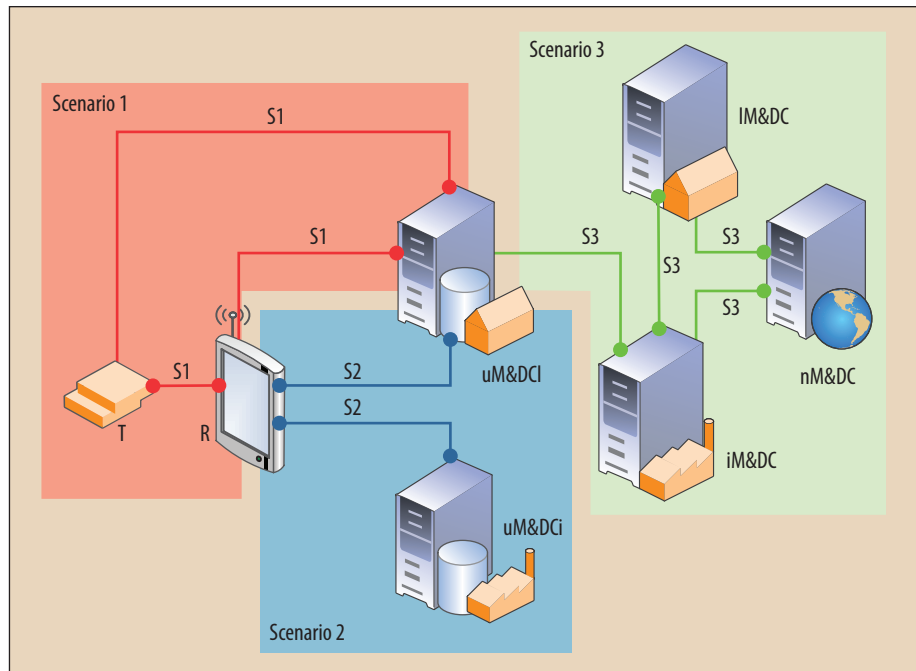


Figure 2. Three cyberentity interaction scenarios.

legal, R will transmit T and R's authentication operators to uM&DCI for identify declaration. Next, uM&DCI verifies T and R. Upon ascertaining their validity, uM&DCI transmits a message to T for secret distribution. R then transmits an authentication operator to T for verification. If R is legal, T and R establish mutual trust for secure data access.

Scenario 2: Privacy-preserving data sharing

This scenario involves an interaction between a local and an industrial IoT under the jurisdictions of IM&DC and iM&DC, respectively. These IoTs have independent authority to access R's data fields, and uM&DCI and uM&DCi grant their own access authority to each other without compromising individual user privacy.

Initially, uM&DCI and uM&DCi transmit access challenges to R, which simultaneously communicates with uM&DCI and uM&DCi. R transmits an authentication operator to uM&DCI for verification. If R is legal, uM&DCI will send a data-sharing request to R, which verifies uM&DCI's request. R then communicates with uM&DCi, and they perform similar operations. Once R has obtained data-sharing requests from uM&DCI and uM&DCi, it ascertains whether they seek to access each other's data. If so, R will transmit the shared data to uM&DCI and uM&DCi, respectively. If the data-sharing requests do not match, R will reveal no data.

Scenario 3: Secure access authority transfer

This scenario involves an interaction among a local, industrial, and national IoT. Here, uM&DCI is originally under IM&DC's jurisdiction, from which iM&DC wants

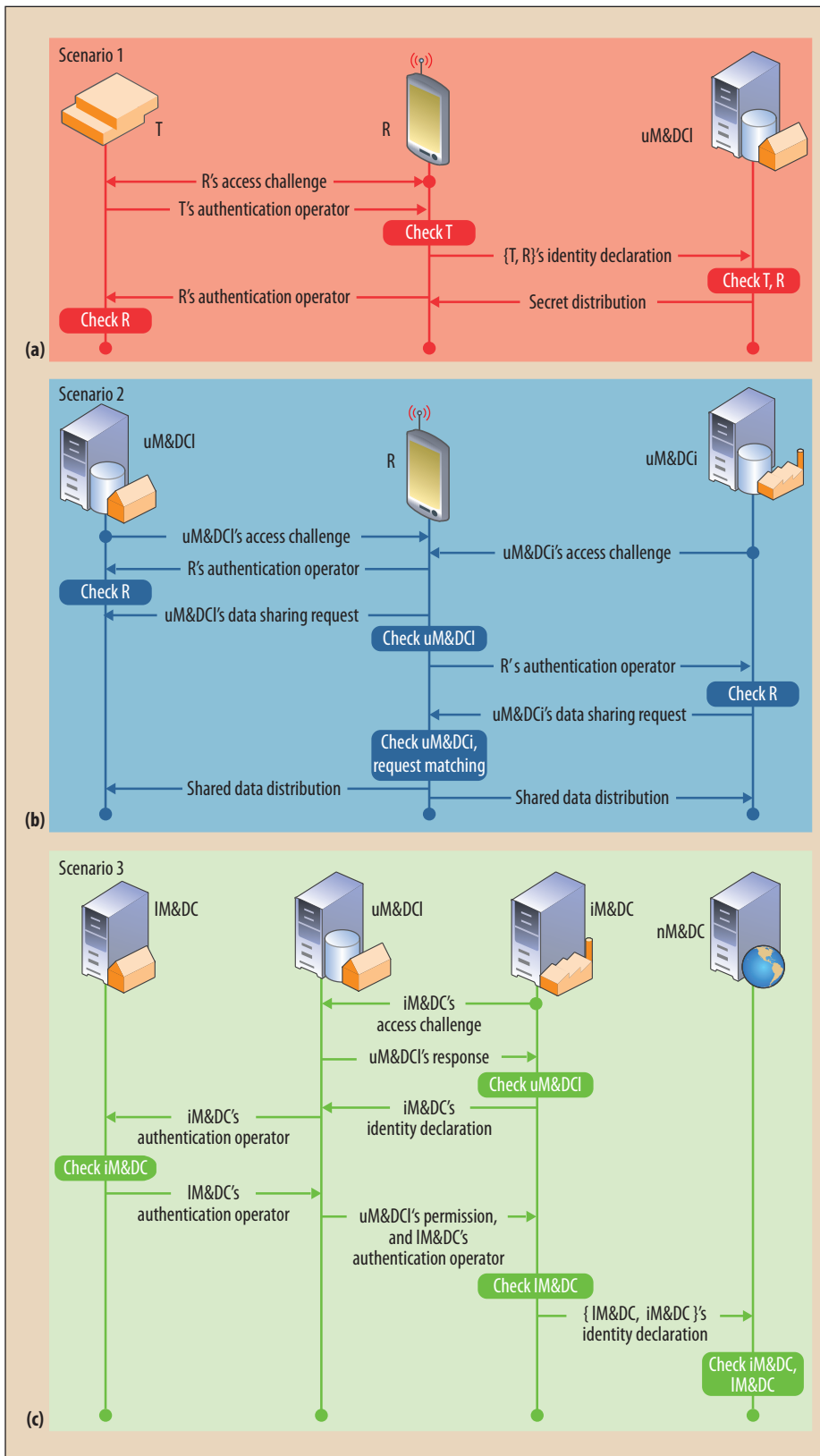


Figure 3. Secure solutions for the three interaction scenarios: (a) secure data access, (b) privacy-preserving data sharing, and (c) secure access authority transfer.

to obtain access authority. IM&DC transfers uM&DCI's authority to iM&DC based on an agreement, and nM&DC performs final verifications on IM&DC and iM&DC.

First, iM&DC transmits an access challenge to uM&DCI for authority transfer, and the latter responds with an authentication operator for iM&DC's verification. If uM&DCI is legal, iM&DC replies with an operator for identity declaration. Next, uM&DCI forwards iM&DC's authentication operator to IM&DC for verification. If iM&DC is legal, IM&DC will reply with an authentication operator to uM&DCI. Thereafter, uM&DCI generates authority permission and forwards IM&DC's authentication operator to iM&DC for verification. If IM&DC is legal, IM&DC and iM&DC will mutually agree on the authority transfer. Next, iM&DC transmits IM&DC and iM&DC's authentication operators to nM&DC for identity declaration. When it ascertains their validity, nM&DC transmits a secret to iM&DC for distribution, realizing the final authority registration.

The proposed solution satisfies four primary security properties.


Session freshness. Pseudo-random numbers and session-sensitive operators such as session identifiers and timestamps serve as access challenges to prevent forward and backward linkability. Even if the cyberentities become corrupted, previous or subsequent sessions will be random.

Mutual authentication. Trusting relationships are

based on preshared secrets such as keys or pseudonyms as well as cryptographic algorithms.

Hierarchical access control. Different access authorities are assigned to cyberentities to protect security. For example, uM&DCI has full authority on T, but R has a limited authority on T. In addition, uM&DCI and uM&DCi have independent access authorities on R's data fields to avoid authority-exceeding violations.

Privacy preservation. Anonymous data-sharing requests preserve privacy; only matched access requests will launch shared data distribution.

As the IoT continues to flourish, offering an attractive future networking paradigm, providing security for cyberentities presents increasingly critical challenges. These emerging challenges include creating more advanced cryptographic protocols, designing appropriate data management architectures, and developing strategies to manage the tradeoffs among security, privacy, and utility. Future research efforts should focus on providing security in heterogeneous network interactions and applying compatible security mechanisms for cross-network authentication and authorization. 

Acknowledgments

This work is jointly funded by the National Natural Science Foundation of China and the Civil Aviation Administration of China (61079019).

References

1. R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, Sept. 2011, pp. 51-58.
2. J. Pan, S. Paul, and R. Jain, "A Survey of the Research on Future Internet Architectures," *IEEE Comm. Magazine*, vol. 49, no. 7, 2011, pp. 26-36.
3. K. McCusker and N.E. O'Connor, "Low-Energy Symmetric Key Distribution in Wireless Sensor Networks," *IEEE Trans. Dependable and Secure Computing*, vol. 8, no. 3, 2011, pp. 363-376.
4. D. He et al., "Secure Service Provision in Smart Grid Communications," *IEEE Comm. Magazine*, vol. 50, no. 8, 2012, pp. 53-61.
5. L. Zhou and H.C. Chao, "Multimedia Traffic Security Architecture for the Internet of Things," *IEEE Network*, vol. 25, no. 3, 2011, pp. 35-40.
6. X. Li et al., "Smart Community: An Internet of Things Application," *IEEE Comm. Magazine*, vol. 49, no. 11, 2011, pp. 68-75.
7. H. Ning and Z. Wang, "Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework?," *IEEE Comm. Letters*, vol. 15, no. 4, 2011, pp. 461-463.

Huansheng Ning is an associate professor in the School of Electronic and Information Engineering at Beihang University, China. His research focuses on the Internet of Things, aviation security, electromagnetic sensing, and computing. Ning received a PhD in information and communication engineering from Beihang University. He is a senior member of IEEE. Contact him at ninghuansheng@buaa.edu.cn.

Hong Liu is a PhD candidate in the School of Electronic and Information Engineering at Beihang University, China. Her research interests include authentication protocol design and security formal modeling and analysis. Liu is a student member of IEEE. Contact her at liuhongler@ee.buaa.edu.cn.

Laurence T. Yang is a professor in the School of Computer Science and Technology at Huazhong University of Science and Technology, Wuhan, China, and in the Department of Computer Science at St. Francis Xavier University, Canada. His research interests include parallel and distributed computing and embedded and ubiquitous/pervasive computing. Yang received a PhD in computer science from the University of Victoria, Canada. He is a member of IEEE. Contact him at lyyang@stfx.ca.



Selected CS articles and columns are available for free at <http://ComputingNow.computer.org>.



CONFERENCES
in the Palm of Your Hand

Let your attendees have:

- conference schedule
- conference information
- paper listings
- and more

The conference program mobile app works for **Android** devices, **iPhone**, **iPad**, and the **Kindle Fire**.

For more information please contact Conference Publishing Services (CPS) at cps@computer.org