Security and Privacy Challenges in Information-Centric Wireless Internet of Things Networks

Boubakr Nour, Kashif Sharif, Fan Li, Yu Wang

Security and Privacy Challenges in Information Centric Wireless IoT Networks

Boubakr Nour, Kashif Sharif, *Member, IEEE,* Fan Li, *Member, IEEE,* and Yu Wang, *Fellow, IEEE*

Abstract—The information-centric networking model uses content as the fundamental element, which can be cached and redistributed within the network. In a large-scale wireless IoT network, this will improve efficiency significantly, but will also render many host-centric security solutions obsolete. This article discusses security and privacy challenges in a merged paradigm.

Index Terms—Information-Centric Networking, Wireless Internet of Things, Security, Privacy

1 Introduction

The current Internet architecture was designed almost four decades ago, to allow two end-hosts share and fetch content using well-known Internet Protocol (IP) addresses. Since that time, the Internet has shown great resilience to the changing requirements of applications. Various protocols and solutions have been proposed to address different user requirements such as mobility, improved content distribution, and most importantly security & privacy. However, humans are not the only users in today's Internet. Mobile and wireless smart devices have become active users, and contribute to the communication process without human intervention. This new model forms the Internet of Things [1].

Internet of Things (IoT) networks are not isolated collection of devices, rather they are use case specific and require continuous connectivity to Internet. Figure 1 shows a generic IoT service structure, where predominantly wireless technologies are used to create access level wireless IoT (WIoT) networks. By integrating IoT devices that can collect/sense data with gateway solutions (applications and customized interfaces) on top of existing infrastructure, a wireless communication model can be realized. However, wireless communication among edge level devices is becoming more prevalent, especially in challenging environments such as smart cities, intelligent vehicle systems, healthcare, smart grids, military, and large industrial sites. The wireless nature of IoT opens newer deployment opportunities for future smart communication systems and can cater to a diverse set of IoT applications. One can find the similarities and roots of such a communication paradigm in Wireless Sensor Networks (WSNs), which (if not identical) had similar goals. This begs the question of using solutions developed for WSNs (in regards to communication, security & privacy) in WIoT. In reality, WIoT is much larger and broader in scope, and WSNs (at best) are a subset of it.

Today's Internet is facing unprecedented challenges in many aspects, where user behavior and application design requirements have moved away from connecting two hosts, towards addressing the content itself. For example, a user is more concerned about watching or sharing a video, and less with the server it is streaming from. This shift from host-oriented towards content-oriented paradigm can be realized by Information Centric Networking (ICN) [2]. In ICN, the content is not requested from a host, but rather from the network. The name of content guides the request to any device which may have a replica of it, thus decoupling the content from its location by using location-independent names. The security mechanisms are applied to the content itself rather than to the communication channel.

Most of WIoT communication patterns such as *sensor content retrieval* and *mobile content updates* (e.g. inquiring the humidity value, or querying report for a patient) are by nature following ICN paradigm, where a device is interested in the content regardless of its location [3]. By decoupling content from its original location, ICN provides

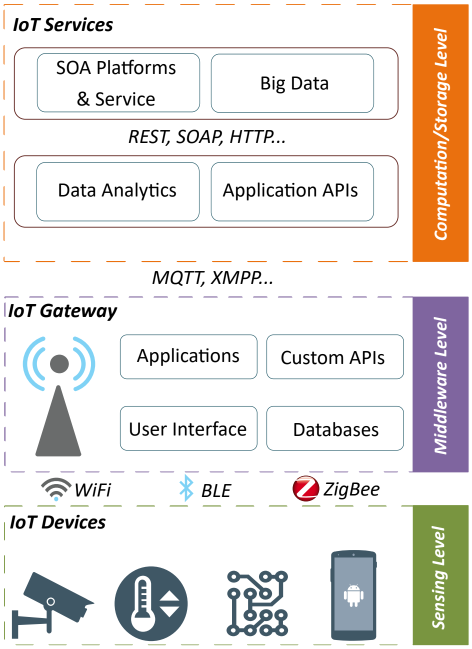


Fig. 1: A general IoT service structure.

B. Nour, K. Sharif, and F. Li are with Beijing Institute of Technology, Beijing, China. Y. Wang is with University of North Carolina at Charlotte, NC, USA.

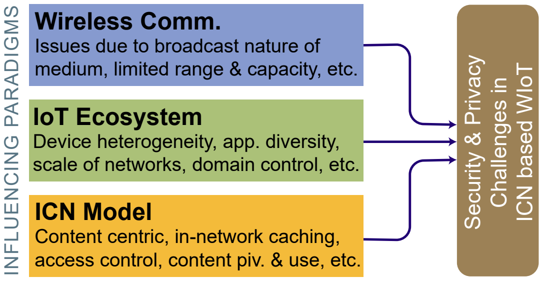

INFLUENCING PARADIGMS
Wireless Comm.
Issues due to broadcast nature of medium, limited range & capacity, etc.
IoT Ecosystem
Device heterogeneity, app. diversity, scale of networks, domain control, etc.
ICN Model
Content centric, in-network caching, access control, content piv. & use, etc.
Security & Privacy Challenges in ICN based WIoT

Fig. 2: The influencing models.

a large naming space with various features embedded in it. IoT applications may benefit from in-network caching of content, its hop-by-hop replication, and availability for re-utilization in the core network. ICN aims to provide better content distribution and content-based security as compared to IP protocol [4]. Hence, ICN design would be a suitable solution for large scale WIoT networks and will improve the ecosystem's efficiency.

Although some efforts have been done to merge ICN with IoT [5], but only at a general architecture level. Furthermore, the security and privacy challenges in such a merged system have rarely been discussed in depth. It is important to understand that ICN based WIoT (ICN-WIoT) security & privacy challenges will be more complex than the individual challenges of WSNs, IoT, or ICN. Figure 2 shows the different influencing paradigms. The security & privacy in ICN based WIoT is effected by: a) wireless nature of the communication medium, b) Inherent limitations of IoT systems, such as heterogeneity, scalability, services, etc., and c) Content centric nature of ICN model. The first objective of this article is to describe the security and privacy goals of WIoT networks and distinguish them from WSNs. Contrary to common misunderstanding the communication models for wireless sensor networks and wireless IoT are different, and hence, the security & privacy issues are also different. The second objective is to discuss the ICN and WIoT merger issues and the existing works and limitations, establishing that there is a dire need for this study. Finally, we identify unique security & privacy challenges for ICN-WIoT networks, then categorize them, and elaborate on the challenge and research opportunities in this domain.

2 Wireless Internet of Things

In order to better understand the security challenges for ICN based WIoT, it is important to first understand the structure, properties, and challenges of wireless IoT networks. To elaborate wireless IoT, we can use wireless sensor networks as a reference model. This is done for two main reasons. a) One cannot deny the conceptual similarities between WSNs & WIoT. Moreover, WSNs have been extensively studied and have become common knowledge in communications research, which makes understanding easier. b) As WSNs have been extensively researched for architecture & security, why not adopt these solutions for WIoT, or why do we need new solutions?

Below we first elaborate the communication model of WIoT, followed by the security challenges.

2.1 Communication Models

Nodes in a WSN are responsible for collecting the sensed data and forward it to the gateway/sink using one-way communication protocols or through data mules (Figure 3a), which is then forwarded to a remote data collection center. Usually, WSN applications are designed & deployed with a specific goal, have well-defined services, and work under a single domain (network & administrator). Hence, they can not be exploited for others uses, while *things* in WIoT can communicate autonomously with each other or with Internet. They can sense/collect data, process, take decisions autonomously, and may be under different domains. WIoT applications are more heterogeneous, designed for general and dynamic services, and can be used for various purposes. Hence, the data collecting and processing services in WIoT are more complex than WSN applications, as shown in Figure 3b. It can be observed that (the largest) difference is in the use cases of IoT, which include healthcare, smart vehicular networks, home & industrial automation, etc. Based on how devices are connected and what type of devices are used, the following classification can be done.

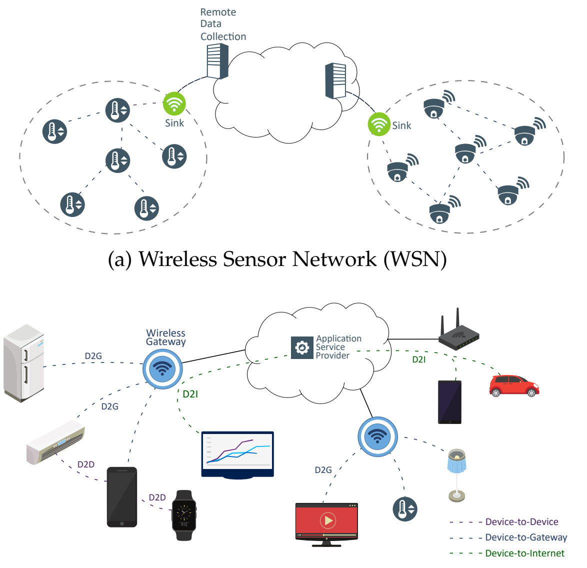
Device-to-Device: Two or more WIoT devices may directly communicate with each other instead of going through an intermediate device/service (e.g., smartwatch to mobile phone).

Device-to-Gateway: This model is also known as Device-to-Application-Layer model, where WIoT device connects with an associated service or gateway, that acts as a complete service point. For example, Home Local Gateway may connect with various smart home WIoT devices (temperature controller, security system, etc.), and control them autonomously. Moreover, it may also allow controlling such devices from remote applications on phone via Internet.

Device-to-Internet: In this model, WIoT devices can directly connect to an application running in the cloud to exchange data and receive control messages, e.g. public surveillance cameras can connect through an Access Point (AP) to the cloud for communication. Hence, AP is not a service point (or destination), but rather a connecting point only.

2.2 Security Issues

Data protection, information security, and privacy are considered to be fundamental requirements for IoT services [1]. The security challenges in WSNs have been extensively studied and mostly classified by the layers in Internet stack. The main goals of such networks are: confidentiality of data, availability of nodes, integrity of information, and authentication & authorization of nodes. The same goals and underlying threats may still be applicable in WIoT, but are not limited to these. In WIoT devices are heterogeneous, making device security at the physical level an added goal. An increase in the number of devices, increases the compromisable points. Moreover, with heterogeneity, same security solutions cannot be applied to all devices. They may use different technologies, which can be an added security challenge. Passive monitoring of device communication can create privacy issues. For example, communication with Smart TV can indicate whether a person is at home, hence



(a) Wireless Sensor Network (WSN)

(b) Wireless IoT Network

Fig. 3: Difference in communication models.

knowledge of actual data may not be required to invade privacy.

WIoT devices run complex operating systems, which are developed by different vendors. With the lack of standardization, it becomes a major goal to keep devices patched and updated against new vulnerabilities. This can be further expanded to the reporting of vulnerabilities by users and active updating by vendors. An important objective for this goal is to keep this process automated, as unlike sensor network users, WIoT users can be technically naive, and may never understand that a vulnerable node at their end can compromise a larger network.

In the big picture, WIoT provides a more comprehensive solution to more personal needs of users. Hence, a large amount of data generated by WIoT devices is personal. Most of such data (even if transferred through secure channels) is stored at cloud servers. IoT is not just end-user devices, hence the security of cloud systems becomes an integrated part of system. As compromised WIoT devices can put cloud data storage in jeopardy, similarly security breaches in cloud servers also impact the IoT ecosystem and user privacy.

In summary, some of the main goals of WIoT security and privacy are:

- Inter-operable security solutions, which can be used with multiple physical layer technologies.
- Implementing authentication of data and devices as part of network, and device profiling to identify rogue mobile devices.
- Preserving content and user privacy, considering passive monitoring of wireless communication.
- Using encryption technologies to ensure interoperability among heterogeneous devices, interference-free and authenticated transmission over the wireless communication medium.
- Implementing secure device update mechanisms, by incorporating robust integrity and authenticity checks, and minimizing service outage due to security breaches.
- Designing devices with embedded security hardware to protect from local tampering.
- Reduction in computation and communication overhead created due to complex encryption and authentication/authorization mechanisms respectively.

3 Integrating ICN Architecture in WIoT

In general ICN architecture, communication should be triggered by a consumer node through an *interest* packet containing the name of the desired content [6]. Intermediate ICN nodes forward the interest packets using name-based routing until they reach a replica-node (caching the same content), or the original content provider. As the content in ICN is decoupled from its location, any node in the network may cache and serve it for future requests. This can reduce overhead at producer, avoid the single point of failure, increase data availability, and reduce network load & data dissemination latency. The response *data* packet follows the reverse path as interest, and is guided by Pending Interest Table (PIT) entries, which are made at intermediate nodes while forwarding interest, and removed with data response traversal. The core network aggregates entries based on content name. Packet forwarding is not performed based on IP address, rather the forwarding strategy is built-on content name and the forwarding interface.

Utilizing ICN architecture for wireless IoT networks is not novel. All IoT devices may become producers and/or consumers, depending on their requirements. The interest packets generated for specific content can be forwarded to neighboring devices or gateway nodes, based on the forwarding strategy. The gateway nodes become optimal data caching points, although caching is not limited to them alone. Depending on physical deployment, all WIoT devices may form a physical layer ad-hoc network and participate in forwarding strategy, or be connected in a hierarchical structure with gateway acting as a sole communication point. In reality, WIoT implementation will be a hybrid of both. As shown in Figure 4, WIoT devices form a mesh network of different technologies. Mobile and static devices can connect to each other and to access points simultaneously. APs may also form a wireless backbone across the city, and integrate smart vehicles into the network. Hence, a true collection of *things* to form their *Internet*.

ICN-WIoT Benefits: From an information sharing point of view, ICN paradigm is an ideal solution for WIoT communication. [5] details generic reason for adoption of ICN into IoT systems. Below, we list some of the benefits that ICN has to offer for WIoT communication.

- Scalability: With billions of connected devices, in-network caching & reduced complexity of multi-casting protocols, will allow the desired scalability. Binding requests to data, rather than device, will also reduce the signaling requirements in wireless domain.
- Design & Deployment: The simple data-centric model will allow easier consumer-driven application design with dynamic quality of service (QoS) guarantees (based on content itself), in ad-hoc or infrastructured environment.

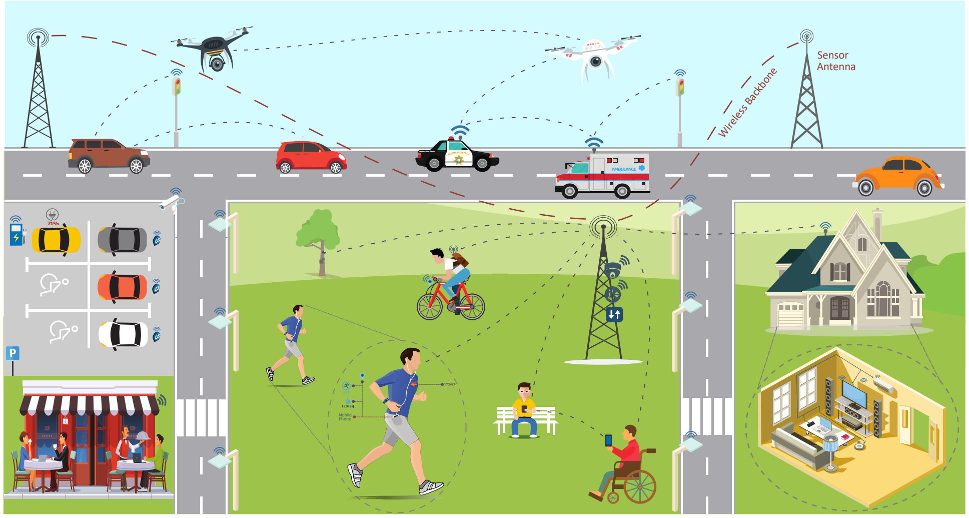


Fig. 4: Integrated Wireless IoT communication.

- Devices: The ICN stack has many optimization services (e.g. QoS, routing, dual addressing, multiple interfaces, etc.) as an integral part, and not add-on protocols as in TCP/IP. This enables the designing of more energy efficient, low-duty-cycle, and compact devices.
- Mobility & Diversity: The consumer-driven ICN designs and the connection-less transport layer means that mobility can be efficiently integrated into all applications and devices. Hence, heterogeneity of devices, manufactures, and communication technologies, will create fewer interoperability issues.
- Security: In contrast to IP based systems, security is implemented as a complete layer in ICN stack. Hence, it will be an integral part of communication and not an optional feature.

Integration Efforts: Several efforts have been made for merging ICN and IoT. [7] focuses on wireless ICN and addresses device-to-device (D2D) communication in virtualized cellular networks. It focuses on content caching and sharing between mobile devices, but does not directly address WIoT security issues. [8] proposes incorporation of sensor networks through gateway based architecture. It considers only ICN related security issues, which are quite limited when WIoT is considered. [9] focuses on distributed secure content sharing in Pub/Sub IoT, and proposes a Ciphertext-Policy Attribute-Based encryption to allow only authorized devices to retrieve the shared cached data. [10] proposes a trust model (without implementation or analysis), to secure ICN-IoT device discovery, naming, and content delivery.

ICN and WIoT still require tremendous research efforts to become practical, but as leading candidates for future Internet architectures, their security & privacy issues are worth exploring to understand the challenges posed by them.

4 Security & Privacy Challenges in ICN based Wireless IoT

WIoT is fundamentally a multi-domain environment with a large number of heterogeneous devices & services. To provide both security and privacy solutions, they have to be integrated into the design of the ecosystem. The use of ICN design as the communication model for WIoT changes most of the fundamental premises of traditional solutions. As the host-centric concept moves to data-centric, the solutions which were designed for Internet stack cannot directly apply to ICN stack. Figure 5 depicts the differences in both stacks, by listing some of the security vulnerabilities. The list is only a sample of possible vulnerabilities. The significant change in layers and their responsibilities have led to changes in vulnerabilities & privacy issues, as some of the attacks can now be launched at multiple levels and with completely different objectives. Moreover, without large scale deployment of ICN solutions, many of the privacy issues may not be visible yet. Hence, it may be premature to list all vulnerabilities or classify them based on where and how an attack can be done.

In the following subsections, we present different aspects of security and privacy challenges of ICN-WIoT systems and discuss the possible issues (using scenario examples), existing solutions (if available), and new research requirements. Table 1 presents a summary of this discussion.

4.1 Wireless Medium & ICN

The physical and Media Access Control (MAC) layers in ICN are still under development, and the role of MAC or IPv6 is not clearly defined. It can be assumed that addressing will be limited to neighbor connectivity, while end-to-end communication will be based on content name, PIT, and Forwarding Information Base only.

Device Level Connectivity: Most of the existing physical layer technologies work in some form of hierarchy, i.e. WiFi: Devices connect to AP only, Bluetooth: Master/Slave connection, etc. These models have been developed to support TCP/IP stack. Exchanging keys to secure communication among two devices is relatively easier. To allow the use of ICN, WIoT devices will have to allow more dynamic communication among them. Consider a scenario with two WIoT devices in each other's range, but connected to different APs. If one requests content that the other has, they can-

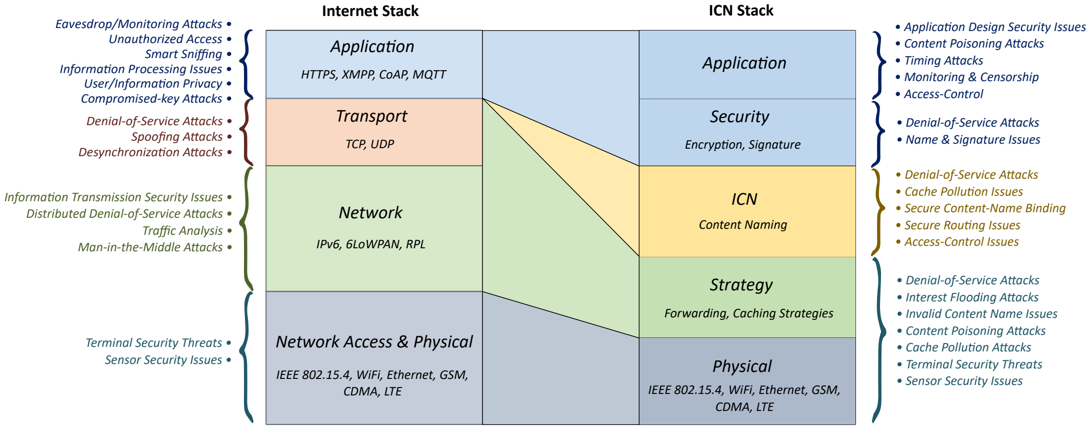

Internet Stack
ICN Stack
Eavesdrop/Monitoring Attacks •
Unauthorized Access •
Smart Sniffing •
Information Processing Issues •
User/Information Privacy •
Compromised-key Attacks •
Denial-of-Service Attacks •
Spoofing Attacks •
Desynchronization Attacks •
Information Transmission Security Issues •
Distributed Denial-of-Service Attacks •
Traffic Analysis •
Man-in-the-Middle Attacks •
Terminal Security Threats •
Sensor Security Issues •
Application
HTTPS, XMPP, CoAP, MQTT
Transport
TCP, UDP
Network
IPv6, 6LoWPAN, RPL
Network Access & Physical
IEEE 802.15.4, WiFi, Ethernet, GSM, CDMA, LTE
Application
Security
Encryption, Signature
ICN
Content Naming
Strategy
Forwarding, Caching Strategies
Physical
IEEE 802.15.4, WiFi, Ethernet, GSM, CDMA, LTE
• Application Design Security Issues
• Content Poisoning Attacks
• Timing Attacks
• Monitoring & Censorship
• Access-Control
• Denial-of-Service Attacks
• Name & Signature Issues
• Denial-of-Service Attacks
• Cache Pollution Issues
• Secure Content-Name Binding
• Secure Routing Issues
• Access-Control Issues
• Denial-of-Service Attacks
• Interest Flooding Attacks
• Invalid Content Name Issues
• Content Poisoning Attacks
• Cache Pollution Attacks
• Terminal Security Threats
• Sensor Security Issues

Fig. 5: Host centric & Information centric stack, with some security and privacy issues.

not take benefits of ICN paradigm, as the communication will follow a path designed for host-centric system. One of the possible solutions would be a passive broadcast to all neighbors. This leads to the requirement of efficient local group encryption schemes. Similarly shared but secured broadcast channels among neighboring devices should be established. However, key management and distribution should not be at the cost of increased communication overhead.

Single Interface: The interface of WIoT devices is represented by a single identifier, be it MAC or IP. Using this with the forwarding principle of ICN creates a major security challenge. Consider a scenario, where an AP or backbone device in WIoT ecosystem aggregates interest requests. The aggregated PIT entry maintains a list of all interfaces which receive the interest requests. Here, all requests will have the same interface, as a single antenna receives them, and in most cases forwards them. Hence, a single malicious response can remove the PIT entry for all requesting WIoT devices. This creates a serious security breach and needs a fundamental design change in ICN model. Possible solutions may include schemes that authenticate neighbor devices before processing their interest/data packets. Another direction is to use a binding mechanism for MAC wireless address with interest packets in the forwarding plane, to track per hop flow of packets. The scalability of such solutions is extremely critical, as dozens of WIoT devices can be found in close vicinity, and tracking all packet flows or authenticating all neighbors may not be possible due to constrained resources.

4.2 Data Protection

Whenever data is published by a WIoT device, it has to be secured. The simplest solution is to encrypt and sign it. Data stored locally can be encrypted by local keys, but this adds to the processing requirements of the device. On the other hand, data once transmitted, needs to maintain its confidentiality and integrity [11].

Data Confidentiality: The data generated by a personal WIoT device may be sensitive, which will require proper encryption. The challenge is the key selection. Unlike IPSec, where a tunnel between two hosts is created, in ICN systems, the same data packet can be cached and distributed multiple times. Hence, the consumer or provider is not always known. The key exchange mechanism has to address this challenge. In the same scenario, if the data is made confidential, there is a possibility that neighboring WIoT devices can still infer the type, size, and other properties. This information may be compromised by the content name in data packets, which are used for forwarding. Hence, either the names should be encrypted (which itself is a challenge) or non-descriptive names should be used (which is a violation of ICN principles). Hence, secure, resistant, and distributed content-name binding mechanisms are essential. Hashing of names can also lead to complex look-up schemes (as compared to prefix matching), which may create a scalability challenge on its own.

Data Integrity: As the wireless environment opens the possibility of malicious nodes generating fake data, efficient signature mechanisms are required, which can ensure that the data has not been tampered with, and is delivered from a legitimate producer or cache. Furthermore, these mechanisms (data validation or signature verification) have to be present at every forwarder and not just at consumers. Replay attacks can be a major challenge here, which will require per packet data integrity. A possible solution can be to generate signatures using time stamp and nonce, so that the message cannot be replayed. Moreover, generation of signatures for each packet must be efficient, so that devices which generate new content frequently are not overburdened.

4.3 Content Caching

Cache polluting and cache poisoning, are two main concerns, which have been studied to some extent in literature, but not from WIoT perspective [12]. We classify the problem as follows:

AP Caching Vulnerability: The general model of WIoT as shown in Figure 4, uses APs to connect devices and form a backbone. This makes them prime candidates to become cache stores. However, this also makes it easier for malicious devices to pollute the caches. The content is cached (in limited memory space) based on its demand. Generally, more *interest* packets for a specific content means more demand, which will force other content (with less demand) to be expunged. As the identity of interest originator is not known at intermediate nodes, hence it is difficult to filter requests which create fake demand. Moreover, malicious nodes can generate fake content, which AP's can cache without knowing its integrity. Integrity checks at each AP cache overburden it, while lack of it will allow fake content reaching consumers, which in response triggers a flood of interests. In such a borderless ecosystem, a new business model based on Blockchain may prove extremely useful. It can be utilized by producers to generate immutable original content, hence fake content from a fake source can be easily verified. Moreover, smart contracts can be used to enforce copyright laws for propitiatory content, which is yet another dimension of security & privacy.

Illegal Cache Stores: A per ICN principle, any device can cache data, and can later provide it to consumers. The content discovery protocols require an in-built mechanism to determine, if the content is being provided by a trusted store, especially in a public WiFi environment. Moreover, obtaining trust-able content from an untrusted store also requires further investigation. This problem gets compounded by the fact that not all nodes should be allowed to cache. Producer devices may have dynamic agreements with cache points to store data, but cannot restrict others from caching. This problem is still open for research, and perhaps can be addressed using smart contracts among devices and content producers. This may not require a complete blockchain solution, but data producers and cache stores (IoT gateways) can enter into an agreement on caching prior to publishing. This can further help in verification of a legitimate source of data other than producer.

4.4 Access Control

Access to devices and access to data are two different issues. Device access should be resolved at physical layer, while data access requires security and application layer involvement in ICN stack [13].

Data Access: Access to published content is an existing challenge in ICN but is drastically increased in WIoT, due to a large number of devices and nature of content. The data distribution is a lower layer functionality in ICN devices, which does not require application involvement. Moreover, the cache stores do not restrict access to data. Hence, dynamic mechanisms to limit content distribution are required. Subscriber-group based mechanisms would be useful in limiting the data distribution, along with blockchain based IoT data access solutions. As ICN uses attributes to name/label content, approaches based on attribute-based encryption [14], [15] can be utilized to enable ciphertext-policy schemes for fine-grained data access control.

User/Device Identity: ICN networks mainly focus on the efficient distribution of content. Hence, the methods to identify users or devices are left to individual applications. Without such identification, access control will be extremely challenging. Physical layer identification may not be sufficient for this purpose. Cross-layer functionality for access control also requires consideration. Although ICN is based on the principle of distributed content, identity management will remain a centralized system.

Policy Enforcement: Content based policies may be a solution, where each content element generated by WIoT device, has a distribution and access policy attached to it. But enforcing such policies and standardizing them is a difficult task, as the WIoT environment is currently unregulated. Dozens of vendors have specialized solutions, with minimum to no interoperability, which makes such policy enforcement difficult. The use of smart contracts from the application layer perspective may enforce policies between entities. However, the implementation of such a mechanism would require Blockchain or distributed ledger technology (DLT) to be a part of overall ICN design. Integrating ICN and Blockchain is a major research direction.

4.5 User Privacy

Assuming that the content or data itself is protected and distribution is controlled, the privacy of devices/users can still be compromised. By inferring information from the wireless medium, malicious nodes can determine the identity and other information of a user. The name of content is usually plain text and self-certified, which can reveal many things, such as type of content, size, how often requested, etc. By passively monitoring the WIoT devices, an attacker can associate them to individuals, and to a great extent determine their behaviors.

Encrypting content names may address this challenge, but will add to the processing overhead on per-hop basis. The use of pseudo names in sensitive requests is a suitable solution, but it will limit the human-readable feature in naming scheme. While the use of pseudonymous authentication may help to preserve user privacy, however, such an implementation in WIoT needs extensive exploration. IoT and blockchain is currently a hot research area, however, most of the solutions are for IoT payment systems [16]. Some major directions concerning blockchain are: a) ICN integration with blockchain, b) reduction in computations requirement for IoT devices, c) Reduction in blockchain communication for wireless devices.

4.6 Encryption & Cryptography

In light of the previous discussion, it is evident that encryption will play an integral role in ICN based WIoT systems.

Encryption Algorithms: In order to protect data, signatures, and content names, encryption algorithms will be decisive in WIoT. Group encryption at link layer will also be required so that all neighbors can communicate in a group. At the same time, WIoT devices are resource constrained. Hence, algorithms have to be highly efficient, while providing the required level of security. Symmetric and asymmetric algorithms for ICN-WIoT also require fresh investigation.

Asymmetric algorithms for encryption may consume more resources, while symmetric algorithms may not be flexible enough to work in ICN-WIoT environment. This requires a detailed analysis of communication architecture for new encryption techniques. Moreover, there is a necessity to develop lightweight and less-resources consuming algorithms, as well as elliptic curve cryptography with resource preservation for lesser complexity.

Key Management & Distribution: One of the major challenges in encryption will be the key exchange methods.

TABLE 1: Future research directions for ICN based wireless IoT.

Aspects	Challenges	Possible Directions
Wireless Medium & ICN	Dynamic key exchange with WIoT connectivity. Forwarding multiple requests with a single Wireless interface.	Secure passive broadcast communication channels. Authenticating request generators or authenticating requests. Mapping MAC Wireless interface with forwarding plane. Localized group encryption schemes. Efficient network creation and device profiling techniques.
Data Protection	Selecting encryption key for data to be distributed. Mitigating fake content with valid signature. Ensuring data is generated by legitimate producer.	A secure, resistant, and distributed content-name binding mechanism. Data validation & signature validation. Scalable name hashing techniques. Efficient signature generation mechanisms to avoid replay attacks.
Content Caching	Realistic definition of in-demand content. Mitigating fake interest demands. Pollution of cache store at APs. Validation of cache stores. Validation of secrecy of correspondence through transparent caching. Restricted caching. Revenue models for in-network caching.	New business models enforcing caching rules based on smart contracts. Including caching and data publishing policies in data packets. Blockchain based content and producer verification. Smart contract based authorization of cache stores.
Access Control	Generating access control rules based on content names dynamically. Employing access control mechanism at cache store level. Identifying user/device at network layer. Enforcing access policies for heterogeneous devices.	Compound key based access control. Subscriber-group based encryption. Use of smart contracts. Attribute based access control policies and encryption. Centralized identity management in a distributed ICN structure.
User Privacy	User identity tracking and monitoring based on content name at network layer. Censorship risk and identity tracing in IoT payment services.	Use of encrypted names. Use of pseudo names in sensitive requests. Pseudonymous authentication. Blockchain based privacy preserving schemes. Techniques for obscuring device to packet relationship.
Encryption & Cryptography	Support of authenticated queries without identifying who requests/provides content. New schemes to overcome resource-constrained WIoT devices. Keys pre-distribution using symmetric cryptography. Signature Authenticity Trust Management.	Lightweight and resources conserving encryption algorithms. Elliptic curve cryptography with lesser complexity. Attribute-tree based authenticated requests. Scalable key distribution & trust management models.

Unlike traditional networks where two parties communicate, ICN can have same content packets delivered to several consumers. Thus the public-private key mechanism for such communication is difficult to implement without compromising the efficiency of ICN. Moreover, WIoT devices will work in groups, hence key distribution will have to be more group-oriented and less host specific. [9] have suggested new key chain mechanisms for encryption & decryption. These are mostly related to data itself, but more efficient solutions are required such as attribute-tree based authentication, scalable key distribution, and trust management methods, which can secure the signatures and name without creating overhead for WIoT devices or violating ICN primitives.

5 State of ICN Implementations

There are two main implementations available for ICN: Named Data Networking (NDN), and Content-Centric Networking (CCN). These are designed for general communication networks, and not specifically for WIoT systems. Both use similar (not completely identical) cryptographic content signature for data verification. Each packet contains a signature of name and content, as well as information about the used key to verify the signature. This mechanism only addresses one element in the broader security and privacy requirements. [17] tries to implement end-to-end secure communication in CCN, but requires every consumer to communicate individually for keys. This creates additional overhead (especially for WIoT) and negates the caching and aggregation benefits. [18] proposes network-layer trust management to mitigate content poisoning attacks. It uses binding rules, verified by each node before cache operation, adding delay and overhead. [19] presents an NDN schematized trust model for data authentication, signing, and access control for consumers and providers. Trust rules define associations between content name and its keys, while trust anchor builds a chain of trust between consumer & producer. It addresses part of the desired security & privacy objectives. Efforts have been made in [20] to port NDN for IoT, however, this solution does not address the security challenges as detailed in this article.

6 Conclusion

ICN and IoT (predominantly wireless at device and edge level) will be two major architectures for future Internet. ICN addresses the core communication paradigm, while WIoT defines the pervasive integrated digital world. Both of these have not been widely or commercially deployed, which is prime time to incorporate what research community has learned from decades of host-centric communication evolution. Security and privacy has been a major challenge in the past, and this article addresses the same in hybrid ICN-WIoT environment. The content centric nature and the wireless domain of IoT drastically changes the way security solutions have been designed earlier, thus they should become part of architecture rather than add-on modules.

Acknowledgments

The work of F. Li is partially supported by the National Natural Science Foundation of China No. 61772077, 61370192, and the Beijing Natural Science Foundation No. 4192051. Drs. Sharif and Li are co-corresponding authors.

References

[1] I. Yaqoob *et al.*, "Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 10–16, 2017.

[2] G. Xylomenos *et al.*, "A survey of information-centric networking research," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 1024–1049, 2014.

[3] B. Nour *et al.*, "A survey of Internet of Things communication using ICN: A use case perspective," *Computer Communications*, vol. 142-143, pp. 95–123, June 2019.

[4] R. Tourani *et al.*, "Security, Privacy, and Access Control in Information-Centric Networking: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 566–600, 2018.

[5] M. Amadeo *et al.*, "Information-Centric networking for the Internet of Things: Challenges and opportunities," *IEEE Network*, vol. 30, no. 2, pp. 92–100, 2016.

[6] B. Nour *et al.*, "M2HAV: A Standardized ICN Naming Scheme for Wireless Devices in Internet of Things," in *International Conference on Wireless Algorithms, Systems, and Applications (WASA)*, Springer, 2017, pp. 289–301.

[7] K. Wang *et al.*, "Information-Centric Wireless Networks with Virtualization and D2D Communications," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 104–111, 2017.

[8] S. S. Adhatarao *et al.*, "ISI: Integrate Sensor Networks to Internet with ICN," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 491–499, 2018.

[9] R. Li *et al.*, "A Distributed Publisher-Driven Secure Data Sharing Scheme for Information-Centric IoT," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 791–803, 2017.

[10] S. Sicari *et al.*, "A secure ICN-IoT architecture," in *International Conference on Communications Workshops (ICC Workshops)*, 2017, pp. 259–264.

[11] Z. Zhang *et al.*, "An Overview of Security Support in Named Data Networking," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 62–68, 2018.

[12] Y. Yu *et al.*, "Content protection in named data networking: Challenges and potential solutions," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 82–87, 2018.

[13] L. Wang *et al.*, "Securing named data networking: Attribute-based encryption and beyond," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 76–81, 2018.

[14] Y. Zhang *et al.*, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2130–2145, 2018.

[15] Q. Han *et al.*, "Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things," *Future Generation Computer Systems*, vol. 83, pp. 269–277, 2018.

[16] F. Gao *et al.*, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE Network*, vol. 32, no. 6, pp. 184–192, 2018.

[17] C. A. Wood *et al.*, "Flexible end-to-end content security in CCN," in *IEEE Consumer Communications and Networking Conference (CCNC)*, 2014, pp. 858–865.

[18] C. Ghali *et al.*, "Network-layer trust in named-data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 5, pp. 12–19, 2014.

[19] Y. Yu *et al.*, "Schematizing trust in named data networking," in *ACM International Conference on Information-Centric Networking*, 2015, pp. 177–186.

[20] M. Amadeo *et al.*, "Named data networking for IoT: An architectural perspective," in *IEEE European Conference on Networks and Communications (EuCNC)*, 2014, pp. 1–5.