Privacy and Security Challenges in Internet of Things

Manik Lal Das

DA-IICT, Gandhinagar, India
maniklal_das@daiict.ac.in

Abstract. Internet of Things (IoT) envisions as a global network, connecting any objects around us, ranging from home appliances, wearable things to military applications. With IoT infrastructure, physical objects such as wearable objects, television, refrigerator, smart phones, supply-chain items and any objects across the globe would get connected using the Internet. Sensing, radio waves, mobile technology, embedded systems and Internet technology are promising actors which play significant roles in IoT infrastructure. Security and privacy issues in IoT scenarios would be much more challenging than what is been used in the conventional wireless scenarios. In particular, the constrained environments require lightweight primitives, secure design and effective integration into other environments in order to see IoT in its desired shape. In this paper, we discuss security and privacy challenges in IoT scenarios and applications with special emphasis on resource-constrained environments' security objectives and privacy requirement. We provide different perspectives of IoT, discuss about important driving forces of IoT, and propose a generic construction of secure protocol suitable for constrained environments with respect to IoT scenarios and applications.

Keywords: Internet of Things, Sensor networks, RFID system, Mobile communications, Security, Privacy.

1 Introduction

The term *Internet of Things* was introduce by the Auto-ID Center in 1999 [1]. After a decade, in 2009, European Commission action plan envisioned "Internet of Things" as a general evolution of the Internet *from a network of interconnected entities (e.g., PC-based LAN, Personal Digital Assistance) to a network of interconnected objects (e.g., household items, consumer electronics)* [2]. With Internet of Things (IoT) infrastructure it is aimed that the Web of world would get connected to all physical objects across the globe, ranging from home appliances, consumer electronics to chemical reactors, military equipments and so on. While connecting these objects (a.k.a. *things*) the Internet would act as the main communication backbone, supported by Bluetooth, Radio waves, Near Field Communication (NFC) as other communication mediums to connect each and every object around us [3]. Embedding technologies such as RFID

R. Natarajan et al. (Eds.): ICDCIT 2015, LNCS 8956, pp. 33–48, 2015.

(Radio Frequency Identification) tags, sensing devices, smart phones are de-facto driving forces in IoT infrastructure along with the conventional PC-based computing environments. Roughly, IoT is an integration of several complementary technological advancements aiming at bridging the gap between the Web of world and the physical world. For example, assume that smart refrigerator is sensor (and reader) enabled, where items inside the refrigerator are RFID tag-enabled. The refrigerator (or items inside it) can be monitored from office or from a shopping complex with the help of a handheld devices (e.g. smart phone). One could also monitor (and control) the status of air conditioning machines at home, door safety, vehicles, and so on, remotely through these resource-constrained systems. Smart energy, intelligent communications, machine-to-machine collaboration, smart home, all these can be realized through IoT infrastructure. Naturally, sensor networks, RFID systems and mobile communications found huge applications in IoT infrastructure. A typical view of IoT scenarios and applications is shown in Figure 1.

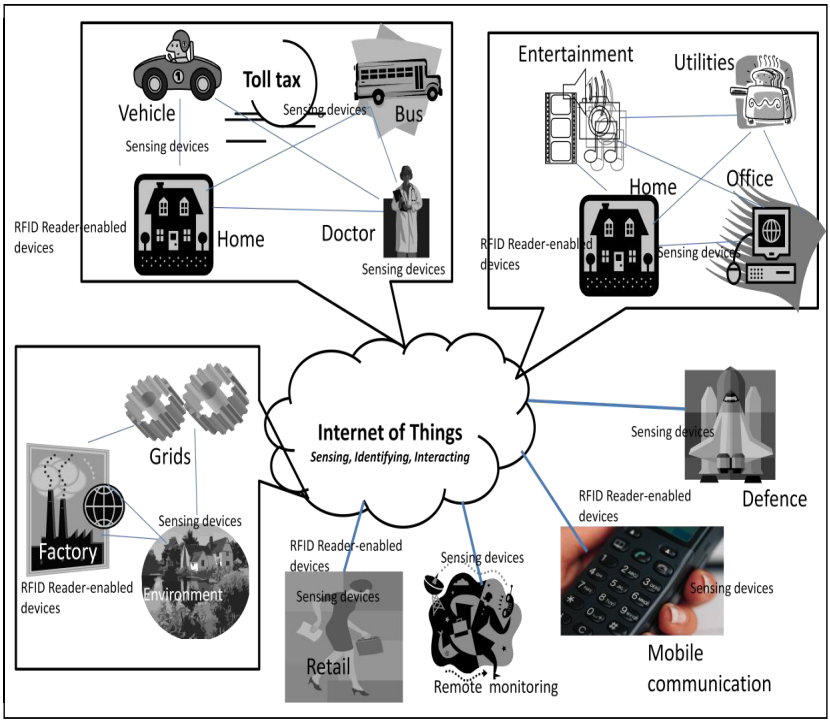

Fig. 1. *Internet of Things* Scenarios and Applications [4]

Wireless Sensor Networks (WSN) [5] has found enormous applications due to its ubiquitous nature, easy deployment and the range of applications they enable.

Networks of thousands tiny sensing devices which have low processing power, limited memory and energy, provide an economical solution to some challenging problems such as military surveillance, real-time traffic monitoring, building safety, wildlife monitoring, measurement of seismic activity and healthcare applications. In the context of IoT, WSN should not be limited with a single or homogeneous application, instead, WSN will act as clusters to manage heterogeneous applications.

RFID system seems to occupy significant places in IoT infrastructure. With RFID tags millions of tiny objects (e.g., books, consumable items, supply chains) would get connected to readers, and then through reader it can connect to Web of world. Typically, an RFID system consists of a set of tags, readers and a back-end server. In IoT scenarios, RFID-enabled things require to talk to other things such as sensors, mobile devices and embedded systems through RFID reader-enabled capability (assume that other devices are also RFID reader-enabled).

The advances of mobile technology (e.g. 4G, 5G) with apps world have made Web of world smart enough to extend its reach to more and more physical objects. Nowadays, mobile technology is used not only for voice communications or text messaging but also mobile phone equipped with available resources acts as a resourceful computing-communicating device for secure billing, trading, content up/downloading and so on. Furthermore, mobile technology helps in connecting sensing/tags-enabled things much easier than the conventional Internet based client-server model.

Other embedding systems, systems-on-chip, and Robotics technology can also contribute enormously in IoT applications. Constrained Application Protocol (CoAP) [6] is a timely designed web transfer protocol for use of these constrained environments. CoAP is an application layer protocol that translates to HTTP for integration with the existing Web while meeting specialized requirements such as multicast support, very low overhead and simplicity for constrained networks (e.g., 6LoWPAN [7]). It is prudent that these constrained environments require need-based security and privacy services to resist potential attackers from controlling their applications. We note that the security requirement varies from application to application. The security primitives used in constrained environment should not consume expensive computational and communication cost. In addition, the integration of these constrained devices along with conventional computing model requires strong security and privacy support in IoT scenarios and applications.

Our Contributions. In this paper, we discuss the security and privacy issues of IoT scenarios and applications. The discussion takes us through the different perspectives of IoT, security and privacy requirements, and important actors of constrained environments in IoT infrastructure. We present a generic construction of secure protocol suitable for constrained environments in the context of IoT. The security goals of the protocol are mutual authentication, key establishment, data confidentiality under the shared key and identity protection. We show how the proposed construction can preserve privacy of the sender and intended security services under an adaptive adversarial model.

Organization of the Paper. The remainder of the paper is organized as follows. Section 2 provides some preliminaries. Section 3 discusses about important actors of IoT. Section 4 presents our generic construction of protocol suitable for constrained environment with respect to IoT scenarios and applications. Section 5 gives the adversarial model. We conclude the paper in Section 6.

2 Preliminaries

2.1 Perspectives of Internet of Things

Technological perspectives. In all terms such as hardware, software, middleware and communication channels, IoT requires context-based technological advancement, keeping consumers' convenience as the primary concern. This leads to a number of issues such as upgrading, migrating, compliance and/or deleting existing technology appropriately and integrating new technology wherever needed, without affecting much impact on service provider and service consumer, based on application requirement. Security, privacy, trust relationship, ownership of data as well as service for Cloud computing, machine-to-machine computing, all these are important concerns that open up significant challenges and opportunities to manufacturers, developers, service providers and service consumers. Embedded devices, handheld devices, RFID tags-readers, smart tokens, sensors, robotics, service-on-chip, nanotechnology and near filed connectivity technologies are to have rapid change in technological advancement. As a result, realization of IoT can be seen as a paradigm shift in all sectors of technological front, which makes significant changes in organizational and societal progress.

Business perspectives. IoT has a wider spectrum of business goal than what Internet-based applications can support these days while writing the paper. Tremendous potential for electronic business has already been arrived, and that is going to scaled up in multiple folds in IoT scenarios. Different countries' strategic drivers require to discuss with standardized forums (e.g., IEEE, ISO/IEC, IETF, SWIFT, ITU) in order to formulate an acceptable business policy that would be applicable to IoT infrastructure. The factors that could work for adopting IoT in industry are Standards, specification, compliance, interoperability, integration, security, privacy, trusts, and ownership. Roughly, the maximum beneficiary of IoT infrastructure is industry itself. Therefore, consumers' privacy, application providers' data protection, service providers' business interest, countries' Information Technology Act compliance, export-import laws are some crucial concerns that need to be addressed globally by research and scientific communities in consultation with Governments and industries.

Economic perspectives. The economic perspectives of IoT offer two kinds of incentives - one to consumers and other to suppliers. On one hand, consumers will directly benefit from IoT infrastructure in terms of optimal time management (e.g. connecting home appliances to office premises), greater flexibility (e.g. anytime-anywhere service), effective security (e.g. door/vehicle-lock/unlock alarm to mobile handset carrying by a person), and increasing revenue (e.g. smart

energy, smart transport, smart shopping). On the other hand, suppliers will benefit by generating revenues in terms of smart services, smart devices and smart technology to assess vulnerabilities and solving them for consumers satisfaction. Small scale service providers can use third party infrastructure for resource sharing/pooling, and large scale providers can make best use of small industries' services.

Human perspectives. Intellectual property, technologies, and information on core processes reside in human minds can be used in IoT in a controlled way depending upon consumers and suppliers requirement. With IoT, things around us could distribute risks far more widely than conventional Internet-based computing environment. Security and privacy of objects could pose a serious threat to some application, and manufacturers could act a single source and/or a single point of failure for mission-critical application. Trust deficiency, inter-dependency and (in)competitive advantage among stake holders of business processes will consume more than expected efforts for IoT to take its desired shape in our modern society. Perhaps, to the best of author's knowledge, this is one of the main reasons why till date individuals, organizations, and Governments are unprepared (or under prepared) for adopting IoT as a global network connecting each and every object across the globe.

In order to provide intended supports towards these perspectives, IoT infrastructure requires to address some of the major challenges [8], [4] as follows.

- Standards: Standards and specifications by international forums are the foremost requirements in order to see IoT in its desired shape. Although European communities have been investing significant efforts for making IoT mission successful, a collective effort by IEEE, NIST, ITU, ISO/IEC, IETF, SWIFT and other standardized body could probably make this mission faster, effective, and implementable
- Identity management: In order to integrate trillions objects in IoT infrastructure, managing identities of objects is a major task in IoT. Both addressing and uniqueness issues have to be addressed suitably. Some existing technologies, such as smart cards, RFID tags [9], IPv6 are going to play important roles for identifying (and addressing) objects in IoT infrastructure.
- Privacy: One of the major challenges in global acceptance of IoT is the privacy of objects, where the privacy issue involves object privacy, location privacy, and human privacy.
- Security: In IoT, the primary means of communication channel is the Internet. Therefore, IoT applications must be safeguarded from both passive and active attackers. In addition to Internet security, IoT infrastructure should provide Intranet security, data security, software security, hardware security, and physical security.
- Trust and Ownership: IoT infrastructure enables communication among various hosts, intermediate systems and end-entity devices. Therefore, trust at device level as well as at protocol level is a key factor in IoT. At the same time, data ownership is an important concern when one system relies on other in order to serve some designated task.

- Integration: One of the main hurdles of IoT infrastructure is the integration of heterogeneous technologies and devices that linked to the Web of world and the physical world. The factors that need to be resolved at integration stage are computation, bandwidth, storage, interoperability and security.
- Scalability: IoT has a wider spectrum than the conventional Internet of computers. Therefore, basic functionalities such as communication and service discovery along with upgrading/migrating/revoking services to function efficiently in both small scale and large scale environments.
- Regulation: In order to have IoT a reality, regulatory issues are key implementation issues for application and software that use public and/or proprietary technology. Every country has its own Information Technology Act and one can enforce certain regulatory norms before allowing a party to implement some application that has larger interest to its citizens. Roughly speaking, this is perhaps the most crucial concern in many countries in order to agree or disagree on IoT's adoption for future Internet applications.

2.2 Security and Privacy Challenges in Constrained System

Embedded devices are increasingly integrated into personal and commercial infrastructures, ranging from home applications to spacecraft applications. When these embedded devices communicate over-the-air, security and privacy issues of entities as well as data are challenging tasks for protecting application from malicious intention. Furthermore, the design criteria of security for embedded systems differs from traditional security design, because these systems are resource-constrained in their capacities and easily accessible to adversaries. When two entities send or receive information using public channels, attackers can eavesdrop/replay/alter messages between communicating entities. Based on application requirement security services such as data confidentiality, integrity, authentication and availability can be enabled in it, but, we note that, the requirement varies from application to application. Data confidentiality protects sensitive information from unauthorized entities. Data integrity ensures that the information has not been altered illegitimately. Entity authentication assures that the information is sent and received by legitimate entities. Another important security property is the availability of intended services. Applications' unresponsive behaviour for just few seconds could be a potential threat to a patient's life in medical application, a disaster to mission critical applications, and also not customer centric for conventional applications. In order to resist potential attacker to deny legitimate customer from applications' services, application must be enabled with appropriate intrusion detection and prevention mechanism.

Embedded devices are small and thus, can be attached to consumer goods, library books, home appliances for identification and tracking purposes. In case of any misuse (e.g. stolen device-enabled items), the terminal can trigger an appropriate message to seller/vendor/owner of the item. The privacy issue could link to object or location. In addition, human privacy may be a concern in embedded system. On one hand, person who carries embedded device could be tracked,

on the other hand, devices' could allow tracing device-enabled objects or person in a controlled way, which could save money, national assets and human lives. We note that the constrained systems should consider suitable primitives (preferably, lightweight primitive), clear design criteria of protocol and implementation aspects with reasonable adversarial assumptions.

2.3 Elliptic Curves Arithmetic

An elliptic curve E over a field F is a cubic curve [10] with no repeated roots. The set $E(F)$ contains all points $P(x, y)$ on the curve, such that x, y are elements of F along with an additional point called the *point at infinity*($\mathcal{O}$). The set $E(F)$ forms an Abelian group under elliptic curve point addition operation with $\mathcal{O}$ as the additive identity. For all $P, Q \in E(F)$, let F_q be a finite field with order prime q. The number of points in the elliptic curve group $E(F_q)$, represented by $\#E(F_q)$, is called the *order of the curve* E over F_q. The order of a point $P \in E(F_q)$ is the smallest positive integer r, such that $rP = \mathcal{O}$. Without loss of generality, the elliptic curve equation can be simplified as $y^2 = x^3 + ax + b \pmod q$, where $a, b \in F_q$ satisfy $4a^3 + 27b^2 \neq 0$, if the characteristic of F_q is neither 2 nor 3. There are two main operations on elliptic curves, point addition and scalar multiplication of point.

Point Addition. The line joining of points P, Q intersects the curve at another point R. This is an interesting feature of elliptic curve and one has to choose a suitable elliptic curve to obtain an elliptic curve group of order sufficiently large to accommodate cryptographic keys.

Scalar Multiplication of a Point. For a scalar n, multiplication of a curve point P by n is defined as n-fold addition of P, i.e., $nP = P + P + \cdots + P$ (n-times). There are fast algorithms [10] for computation of scalar multiplication of point on elliptic curves.

Complexity Assumptions. *Elliptic Curve Discrete Logarithm Problem (ECDLP).* Elliptic Curve Discrete Logarithm Problem (ECDLP) is a standard assumption in which elliptic curve based cryptographic algorithm can rely upon. The ECDLP is stated as: given two elliptic curves points P and $Q(= xP)$, finding scalar x is an intractable problem with best known algorithms and available computational resources.

Decisional Diffie-Hellman (DDH) assumption: Let P be a generator of $E(F_q)$. Let $x, y, z \in_R Z_q$ and $A = xP$, $B = yP$. The DDH assumption states that: the distribution $< A, B, C(= xyP) >$ and $< A, B, C(= zP) >$ is computationally indistinguishable.

Computational Diffie-Hellman (CDH) assumption: Let P be a generator of $E(F_q)$. Let $x, y \in_R Z_q$ and $A = xP$, $B = yP$. The CDH assumption states that: given $< P, A, B >$, it is computationally intractable to compute the value xyP.

3 Driving Forces of Internet of Things

IoT infrastructure requires to facilitate seamless data collection/update between objects with the help of Internet. Sensor networks, RFID system, Smart phone domain, and other embedded systems would have a strong hold in IoT infrastructure, where conventional PC-based LAN/WLAN paradigm remains pivotal functional body that may control other environments suitably.

3.1 Wireless Sensor Networks

In IoT infrastructure, wireless sensor networks (WSN) require interaction with RFID system, handheld devices, and other constrained devices including conventional PC-based LAN setup to reaching out both static and movable objects. WSN consists of several tiny sensing devices and one or more base stations who collect data from sensors as per application's goal. Furthermore, depending on applications' goals, the network adopt cluster-based architecture, where each cluster head is equipped with more resources than sensor nodes deployed in it. Irrespective of cluster-based or non-cluster based architecture, most of the WSN applications require authentication and integrity of data exchanged between sensor nodes and base station. Moreover, some applications (e.g. healthcare) require data confidentiality, privacy preserving, and availability of data in addition to authentication and integrity.

3.2 RFID System

RFID system has found enormous applications in retail, supply-chain, health care, transport, and home appliances. An RFID system consists of a set of tags, readers and a back-end server. A tag is basically a microchip with limited memory along with a transponder. Every tag has a unique identity, which is used for its identification purpose. A reader is a device used to interrogate RFID tags. The reader also consists of one or more transceivers which emit radio waves by which passive tags respond back to the reader. The back-end server is assumed to be a trusted server that maintains tags and readers information in its database. In the context of IoT, RFID-enabled things require to talk to other things such as sensors, mobile devices and embedded systems through RFID reader-enabled capability.

3.3 Mobile System

Mobile technologies (e.g. 3G, 4G) have revolutionized the computing and communicating world. Mobile phones along with Internet have virtually substituted the need of desktop PC in wired or wireless environment. Smart phones equipped with multi-core processors support services such as emailing, trading, video conferencing, social networking and so on. Mobile communication system consists of Mobile station, Base station subsystem and Network subsystem. The network subsystem is governed by other entities like AuC (authentication centre), EIR

(equipment identification register), HLR (home location register) and VLR (visiting location register). The security part of mobile communication is primarily controlled by the network subsystem with the help of these entities. Furthermore, it has been seen that the security algorithm used mobile communication in some cases are proprietary, not available for public scrutiny. In the context of IoT, mobile technology is going to act as an important contact point to other resource-constrained systems (e.g., RFID system, WSN). Therefore, standard and uniform security specification and interoperable standards among heterogenous technologies/devices are an imperative demand in industry for protecting applications from potential adversaries.

3.4 Connectivity Technology

The success factor of IoT primarily relies on the power of Internet technology. Internet technology supports unique addressing for computers on a network. The addressing field is of 128-bit length while using IPv6. In other words, Internet technology has enough space to connect trillions objects by uniquely assigned IP addresses. Internet along with near filed communication (NFC) such as bluetooth, radio waves, infrared can reach out each and every object around us. In addition,low-power wireless mesh networking standard like ZigBee [11] along with IEEE 802.15.4 MAC can connect tiny sensors embedded in low-cost devices. The 6LoWPAN (IPv6 over Low-power Wireless Personal Area Networks) [7] can also run on physical layers and allows for seamless integration with other IP-based systems. Importantly, 6LoWPAN offers interoperability with other wireless 802.15.4 devices as well as with devices on any other IP network link (e.g., Ethernet, WiFi). In summary, these connectivity technologies are adequate in communication strength to connect all objects across the globe. The Figure 2 tries to capture the important actors of IoT infrastructure.

3.5 CoAP-Constrained Application Protocol

Constrained Application Protocol (CoAP) [6] is a recently devised web transfer protocol for use of constrained nodes (e.g., low-power sensors, switches, or valves) in constrained (e.g., low-power, lossy) networks. CoAP translates to HTTP for integration with the existing Web while meeting specialized requirements such as multicast support, very low overhead and simplicity for constrained environments, and machine-to-machine applications. Using CoAP, entities can provide services over any IP network using UDP. Any HTTP client or server can interoperate with CoAP enabled entities by installing a translation proxy between the communicating devices. As a result, CoAP with tiny embedded device has huge potential to integrate other constrained environments with IoT by using Internet. In the context of security, the CoAP supports flexible security services such as no key, symmetric key and public key based DTLS [12], which could provide need-based security layers based on application requirement.

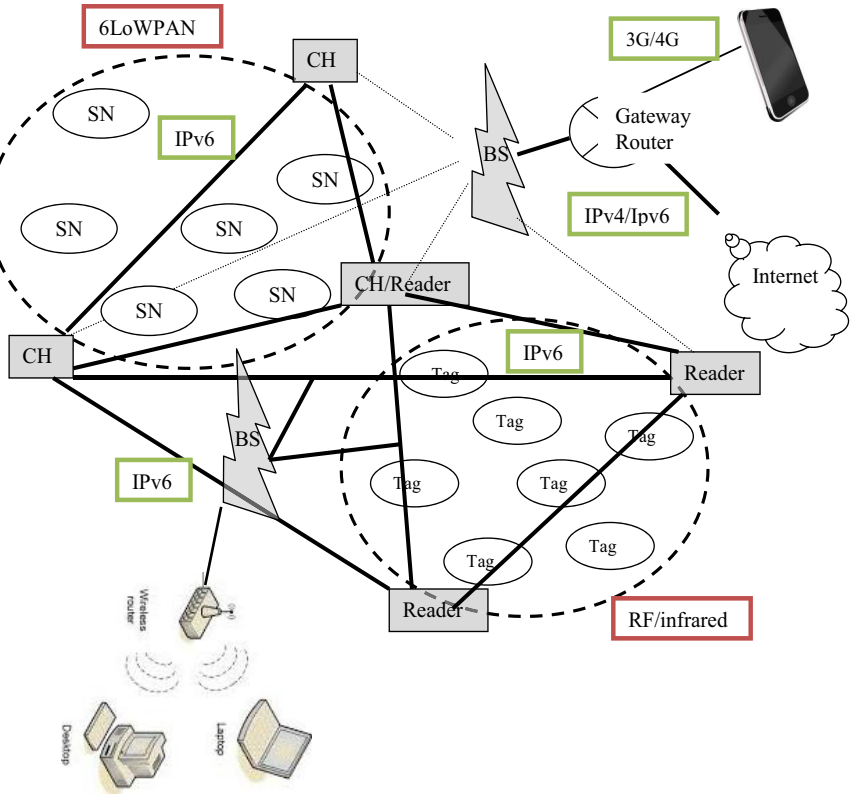

Fig. 2. Constrained environments for IoT Infrastructure

4 Secure Protocol for IoT Applications

A protocol should have precise goal, assumption and clear design principle. The construction that we consider for modelling the proposed protocol has following objectives.

Goals. The protocol aims to provide entity authentication, authenticated key establishment and data confidentiality with a shared key established during the current run of the protocol. The protocol can also support effective privacy of protocol initiator (sender of the proposed protocol).

Assumptions. We consider an adaptive adversary who can gather any number of message exchange between sender and receiver, and add/delete message components. The adversary can also compromise any sender to impersonate a target sender or receiver. We assume that the secret(s) stored in the sending/receiving

devices is not know to the adversary. The protocol resists replay, impersonation, and linkability under standard complexity assumption.

Design Choice. The protocol requires to use public key primitives for strong authentication, key exchange and privacy preserving properties. Based on application requirement, the other properties like anonymity, unlinkability, non-repudiation can be required services. However, we consider primarily the former set of security properties. We use elliptic curve cryptography [10] because of its small key size and other interesting features. Furthermore, standard symmetric key cryptography and pseudo-random function are to be used for data confidentiality and authentication codes generation.

We consider the architecture depicted in Figure 3 for modelling our protocol. The protocol provides a generic sender-receiver communication structure that can be implemented between two communicating entities such as tag–reader in RFID system, sensor node–base station in WSN, mobile phone–base station in mobile scenario and so on. The communication between receiver and proxy server (or between proxy to proxy server) could rely on some standard protocol (e.g. TLS [13]) where certificate-based proxy delegation, revocation and other required security services be enabled in the protocol based on application requirement.

4.1 Generic Construction

The protocol consists of two principal participants - *sender* and *receiver*. The sender could be sensor, mobile station, or tag; and receiver could be cluster head, base station, or reader. The protocol has four phases - system initialization, pre-deployment, authenticated key establishment, and data confidentiality.

System Initialization. The system may consist of many senders and receivers. For the sake of simplicity, we consider the system with many senders and one receiver. The receiver acts as the server's agent (e.g., proxy server) or the server itself.

The setup server chooses a suitable elliptic curve $E(F_q)$ over a finite field F_q where q is a prime number sufficiently large enough to accommodate cryptographic keys. Let $P \in E(F_q)$ be the generator of $E(F_q)$. The parameters $E(F_q)$, q and P are made public. We refer interested readers to [10] for more on elliptic curves arithmetic and properties.

Pre-deployment Phase. All senders and the receiver of the system require to register into the system before deployment. The registration process follows a a secure mechanism by which sending and receiving devices are being personalized with intended security parameters. We assume that a trusted setup server does the personalization process of sender and receiver during their registration.

Sender personalization: The setup server personalizes the sender with a private key $x \in_R Z_q^*$. The corresponding public key X $(=xP)$ is stored in the sender's memory. In addition, the public parameters $E(F_q)$, q and P are also stored in the sender's memory.

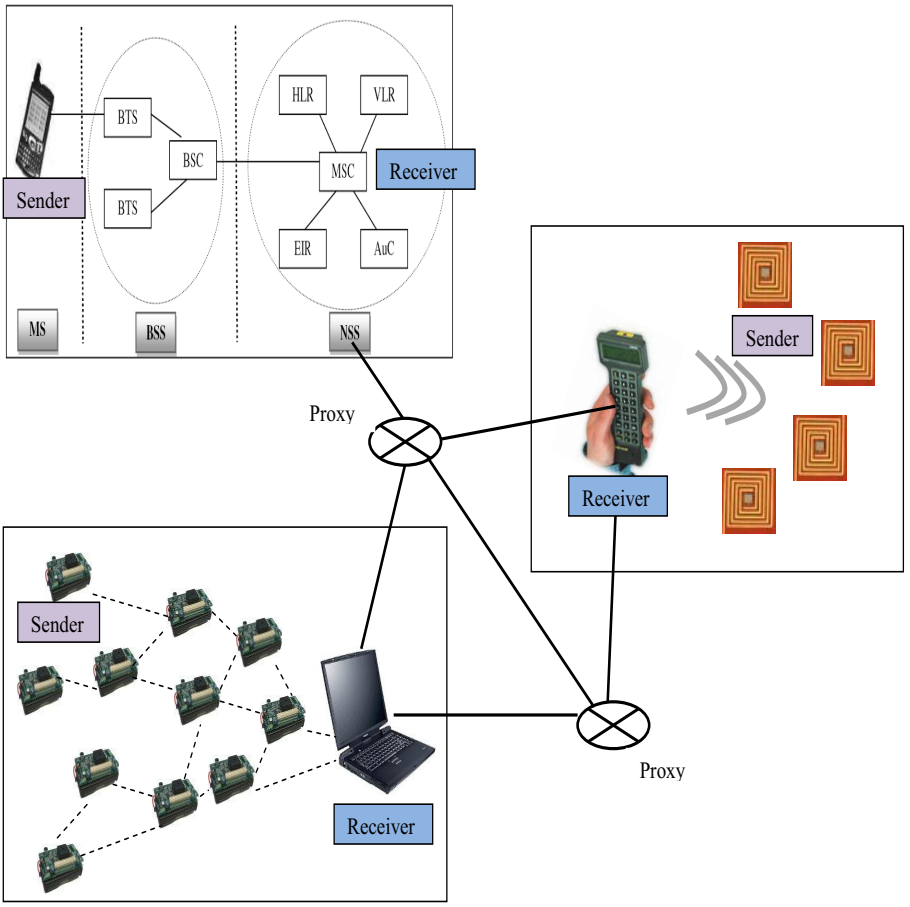

Fig. 3. Architecture considered for modelling the protocol

Receiver personalization: Like sender personalization the setup server personalizes a receiver with a private key $y \in_R Z_q^*$. The corresponding public key Y $(=yP)$ is stored in receiver's memory. The receiver's memory has to be personalized with the public parameters $E(F_q)$, q and P.

We note that X and Y provide identity information of the sender and the receiver, respectively. Furthermore, a sender is also personalized with receiver's public key Y and the receiver is personalized with all senders public keys Xs. It is also noted that the personalization phase is executed for sender/receiver only once before its deployment into the system.

Authentication, Key Establishment, and Data Confidentiality. This phase is invoked as and when sender wants to communicate with receiver. By successful execution of this phase both sender and receiver mutually

authenticate each other. They also establish a shared secret key followed by traffic confidentiality under the shared key. The phase works as follows:

1. Sender selects a random number $n_s \in_R Z_q$, and computes $N_s = n_s P$, $chl = \mathcal{F}(X, n_s, Y)$. The sender sends $< N_s, chl >$ to the receiver.
2. Upon receiving $< N_s, chl >$, the receiver first retrieves X from chl [1]. Then, the receiver checks whether X is a registered entity. If not, the receiver terminates the operation; else, the receiver selects a random $n_r \in_R Z_q$ and computes
   $$N_r = n_r P$$
   $$res = \mathcal{F}(Y, n_r, X)$$
   $$k_r = \mathcal{G}(N_s, y, n_r, X)$$
   $$c_r = \mathcal{H}(X \| Y \| k_r \| N_s \| N_r)$$
   The receiver sends $< N_r, res, c_r >$ to the sender as a response to sender's challenge chl. Here, $\mathcal{F}$, $\mathcal{G}$, and $\mathcal{H}$ are suitable operations/functions (e.g., elliptic curve arithmetic, pseudo-random function).
3. Upon receiving $< N_r, res, c_r >$, the sender retrieves Y from res. If Y is not found in sender's memory, the sender discards the message. If Y is found, the sender computes
   $$k_s = \mathcal{G}(N_r, x, n_s, Y)$$
   $$c'_r = \mathcal{H}(X \| Y \| k_s \| N_s \| N_r)$$
   then checks whether $c'_r = c_r$. If it holds, then the receiver's authentication is confirmed. Now, the sender computes $confirm = \mathcal{H}(k_s \| \textit{ all previous messages})$ and sends $confirm$ to the receiver.
4. Receiver checks whether $confirm = \mathcal{H}(k_r \| \textit{ all previous messages except the last one})$. If it holds, then the sender's authentication is confirmed.

4.2 Security and Privacy Claim

We show how the above construction achieves intended security and privacy goals.

Mutual Authentication. In step 2, the receiver confirms the sender's participation by checking X's presence in its memory, and sender's authentication is confirmed with step 4. In step 3, the sender confirms the receiver's authentication. In step 4, the key confirmation is achieved. It is noted that the authentication of sender and receiver is achieved with a standard message authentication code (i.e., with the pseudo-random function $\mathcal{H}$ and secret parameters).

Key Establishment. After successful run of the protocol, both sender and receiver have established a transient key k_s (*resp.* k_r). Using this transient key they can derive a shared key $SK = \mathcal{H}(X \| k_{s/r} \| Y)$. The shared key SK has input

[1] This requires some additional parameter be communicated along with chl; however, one can use any alternative ways to do this part. We refer readers to [4] for a ready reference.

of the private key, the public key and the transient secrets. Once the session is expired, the transient secrets n_s and n_r get erased from the respective local state of the sender and receiver. This would also enable the protocol in achieving *forward secrecy*, a useful security property required for many applications.

Data Confidentiality. Depending on the nature of applications where resource-constrained devices are being deployed, the sender-receiver communication may require protection from unauthorized access. The sender and receiver can generate their write key $E_s = \mathcal{H}(X\|SK\|SID\|\text{`}sender'\text{)}$ and $E_r = \mathcal{H}(Y\|SK\|SID\|$ `$receiver'$), respectively. Note that the parameter SID is the session identifier. Now, the sender (*resp.*, receiver) can use E_s (*resp.*, E_r) for encrypting data, and thereby, communicating over a secure channel.

Identity Protection. In the proposed construction, the messages exchange between sender and receiver do not leak any identification of sender and receiver. This guarantees the protection of the identities of the communicating parties. This would help in preserving privacy of sender (and also receiver), which is an important feature of many emerging applications.

5 Security Analysis

Adversarial model. An adaptive adversary is considered who can intercept messages between sender and receiver, and can replay, manipulate the message by adding or deleting data in it. The adversary is allowed to run following queries:

- `initialize virtual sender`. on input a sender identity, this oracle personalizes a virtual sender with x^v, X^v, Y as secret parameters and stores other public parameters in its memory. Then, it returns the personalized device to the adversary. Note that the adversary can know the reader's public key with this query, so reader's privacy is not aimed in this case; otherwise, the adversary should not have reader's public key Y. The system may also consider the sending device is tamper resistant, so the stored parameters can not be extracted from its memory. But, this costs more to the applications like RFID and WSN, where number of tags and sensors are large, and therefore, having device tamper-proof is not a practical solution. We assume that by running the `initialize virtual sender` query, the adversary has knowledge of Y. In other words, the privacy of the receiver is not aimed at this adversarial model.
- `response query`. on input $< N_s^v, chl^v >$ with respect to the adversary's controlled device, this oracle returns the tuple $< N_r^v, res_r^v, c_r^v >$ to the adversary if X^v is in receiver's database. If X^v is not found in the receiver's database, it returns $\perp$.
- `auth query`. on input $< confirm^v >$, this oracle returns a bit indicating whether or not the receiver accepts the session of the protocol run that resulted in successful authentication of the sender. If the bit value is 1 then

the receiver has established a session with the sender, whereas, bit value 0 indicates unauthorized attempt and no session has been established with the sender.

- `corrupt query`. on input target device, this query returns x_{target} and Y to the adversary.

5.1 Security experiment

In this experiment, the adversary's goal is to convince the receiver to accept an unauthorized sender. In order to convince the receiver, the adversary requires to compute a valid *chl* and $confirm$ on a target sender, where the target sender has not participated in above queries.

Claim 1. *The proposed construction of the protocol is secure as no polynomial time adversary can establish a session with the receiver with non-negligible advantage in the security parameter used in the initialization phase under standard complexity assumptions.*

The above claim can be proved by the security proof sketch used in [4], [14].

5.2 Privacy experiment

The goal of the adversary in this experiment is to distinguish between two different participating senders. Let us assume that the experiment consists of a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$. The experiment is defined as follows.

$\texttt{Exp}^{b}_{\mathcal{S},\mathcal{A}}(k)$:

1. $b \in_R \{0,1\}$
2. `Setup Receiver`(1^k), where k is the security parameter
3. $g \leftarrow \mathcal{A}^{\texttt{Queries}}(\textit{adversarial capability})$
4. Check whether $g = b$

The challenger $\mathcal{C}$ presents to $\mathcal{A}$ the system where either S_i (if $b = 0$) or S_j (if $b = 1$) is selected when returning a `response` query.

The adversary $\mathcal{A}$ is allowed to query the above mentioned oracles any number of times and then outputs a guess bit g. We say that $\mathcal{A}$ breaks the privacy of the protocol if and only if $g = b$, that is, if it correctly identifies which of the sender was in participation. The advantage of the adversary is defined as $\texttt{Adv}_{\mathcal{A}}(k) = \Pr[\ \texttt{Exp}^{0}_{\mathcal{S},\mathcal{A}}(k) = 1\ ] + \Pr[\ \texttt{Exp}^{1}_{\mathcal{S},\mathcal{A}}(k) = 1] - 1$

Claim 2. *The proposed construction of the protocol preserves privacy of senders as any polynomial time adversary can have advantage in guessing a sender participation negligible (not more than a random guessing) in security parameter k under standard assumptions.*

The above claim can be proved by the security proof sketch provided in [4], [14].

6 Conclusions

Internet of Things (IoT) envisions as a global network, which would connect any objects across the globe through Internet. In addition to conventional PC-based Internet computing, WSN, RFID system, mobile computing are essential

components that would contribute significantly to IoT infrastructure. In IoT infrastructure, these complimentary technologies require to interact each other in order to connect objects around us. As a result, security and privacy of these constrained environments are important concerns in IoT scenarios and applications. We discussed various security and privacy issues pertaining to IoT infrastructure. We have highlighted different perspectives of IoT, discussed about important driving forces of IoT. We then proposed a generic construction of secure protocol for resource-constrained environment in the context of IoT infrastructure. The proposed construction can support authentication, key establishment and data confidentiality security properties. Furthermore, the construction allows to to achieve effective privacy of the communication parties by protecting their identities in message exchange.

References

1. Sarma, S., Brock, D.L., Ashton, K.: The Networked Physical World. MIT Auto-ID Center (2000)
2. European Commission: Internet of Things - An action plan for Europe, http://europa.eu/legislation_summaries/information_society/internet/si0009_en.htm (accessed January 2014)
3. Yan, L., Zhang, Y., Yang, L.T., Ning, H.: The Internet Of Things. Auerbach Publications, Taylor and Francis Group, New York (2008)
4. Das, M.L.: Strong Security and Privacy of RFID System for *Internet of Things* Infrastructure. In: Gierlichs, B., Guilley, S., Mukhopadhyay, D. (eds.) SPACE 2013. LNCS, vol. 8204, pp. 56–69. Springer, Heidelberg (2013)
5. Callaway Jr., E.H.: Wireless Sensor Networks. Architectures and Protocols. Auerbach Publications (2003)
6. Shelby, Z., Hartke, K., Bormann, C.: The Constrained Application Protocol (CoAP). RFC 7252 (June 2014), https://tools.ietf.org/html/rfc7252 (accessed July 2014)
7. Kushalnagar, N., Montenegro, G., Schumacher, C.: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). RFC 4919 (August 2007), http://www.ietf.org/rfc/rfc4919.txt (accessed December 2013)
8. Roman, R., Najera, P., Lopez, J.: Securing the Internet of Things. IEEE Computer 44(9), 51–58 (2011)
9. ISO/IEC 14443-2:2001. Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface
10. Hankerson, D., Menezes, A., Vanstone, S.: Guide to Elliptic Curve Cryptography. Springer (2004)
11. ZigBee Specification, http://www.zigbee.org/Specifications.aspx (accessed December 2013)
12. Rescorla, E., Modadugu, N.: Datagram Transport Layer Security. RFC 4347 (April 2006), https://tools.ietf.org/html/rfc4347 (accessed December 2013)
13. Dierks, T., Rescorla, E.: The Transport Layer Security (TLS) Protocol. RFC 5246 (August 2008), http://www.rfc-base.org/txt/rfc-5246.txt (accessed December 2013)
14. Songhela, R., Das, M.L.: Yet Another Strong Privacy-Preserving RFID Mutual Authentication Protocol. In: Chakraborty, R.S., Matyas, V., Schaumont, P. (eds.) SPACE 2014. LNCS, vol. 8804, pp. 171–182. Springer, Heidelberg (2014)