Chapter

Survey and Analysis of Lightweight Authentication Mechanisms

Adarsh Kumar and Deepak Kumar Sharma

Abstract

Interconnection of devices through Radio Frequency IDentification (RFID) brings enormous applications that are increasing constantly day by day. Due to the rapid growth of such applications, security of RFID networks becomes crucial and is a major challenge. Classical or lightweight cryptography primitives and protocols are the solutions to enhance the security standards in such networks. Authentication protocols are one of the important security protocols required to be integrated before exchange of secured information. This work surveyed the recently developed authentication protocols. Further, classifications, security challenges, and attack analysis are explored. A comparative analysis of different types of authentication protocols explains their applications in resourceful and resource constraint Internet of Things (IoT). Authentication protocols are categorized into: symmetric, asymmetric, lightweight, ultra-lightweight and group protocols. Symmetric and asymmetric protocols are more suitable for resourceful devices whereas lightweight and ultra-lightweight protocols are designed for resource constraint devices. Security and cost analysis shows that asymmetric protocols provide higher security than any other protocol at a reasonable cost. However, lightweight authentication protocols are suitable for passive RFID devices but do not provide full security.

Keywords: authentication, authorization, cost analysis, cybersecurity, lightweight cryptography, primitives, protocols

1. Introduction

Kevin Ashton in 2009 proposed an interconnected network of uniquely identifiable objects, devices, and different types of systems called IoT [1]. Some of the important features of IoT are self-configuration, sensing, ad-hoc networking, automatic identification, etc. [2]. In IoT, each object has a unique address and identification. Here, mostly RFID is preferred for assigning an address and unique object identification. The information, captured by IoT objects, is propagated through the internet to other objects. The information communicated captures the current events and responses. The revealed information further requires human intervention to control the results [3]. Several objects are involved to form the interconnected network: RFID devices, sensors, mobiles, back end storage, etc. Resourceful and resource constraints are the types of IoT devices. In resourceful devices, there are sufficient software and hardware resources. There are some hardware and software resource limitations in resource constraint devices. The role

of the devices changes with the condition. For example, a metro smart card authenticates the passenger at the entry point, the same card authenticates exit after deducting a charge for the travel. Using the same smart card, information of daily passenger traveling systems is stored in a database server and helps in train counting. Library management, supply chain management, and inventory control systems are some of the applications of RFID enabled things. Here, users are validated using authentication protocols. Unauthenticated users are disallowed to enter into the system. The observation system is maintained to analyze the possibilities of intrusions by unauthenticated users.

There are different types of authentication protocols. Cryptographic primitives, like AES, RSA, SHA, etc. are used in resourceful devices for authentication and authorization. Lightweight primitives and lightweight protocols are the different types of lightweight cryptography [4]. Stream cipher, hash function, block cipher, pseudo-random number generation, etc. are included in symmetric primitives whereas asymmetric primitives include discrete logarithmic constructions, number based systems, and curve based cryptosystems. Authentication, yoking, identification, tag ownership protocols, distance bounding, etc. are some classes of lightweight protocols. Up to 30% of gate equivalents (GEs) can be used in resource constraint devices for cryptographic [5, 6]. With the advancement of technology, the GEs also increase [7].

Tags, readers, and data centers are the three types of RFID devices. Information is written over tags and readers are used to read the information. If required, data center is used for storing the information; otherwise, it is communicated to other objects to increase the information availability. The behavior of readers is similar to duplex links. These devices use different procedure for storing data. The tags get power from these devices and have longer information availability range. Tags, passive, semi-passive, active follows the cryptography procedures as implemented [8]. Passive tags do not have their source of power. These tags have low costs and low memory. These are more suitable for short range. Information on these devices is read many times after writing it for once [9–11]. Active tags are more costly, have their battery source, limited battery and communication range. Active or Semi-passive tags show economical to active tags and costlier to passive tags [12, 13]. These three tags are used in different applications. Semi-passive tags are mainly used in applications such as alarm systems, thermostats, etc. Active tags are used in applications meant for animal or person tracking, health care systems, etc. Supply chain management, smart cards, etc. are some applications of passive tags [14–29].

1.1 Chapter organization

The rest of the chapter is organized as follows: Section 2 states the important security parameters required to analyze the authentication protocols. Section 3 introduces the classifications of recently developed authentication protocols [30]. Lightweight authentication protocols are discussed in section 4. Section 5 presents group authentication protocols. In this section, authentication protocols are classified, explained and analyzed from important attacks. Comparative security and cost analysis of surveyed authentication protocol is presented in section 6. Finally, conclusive and future scope remarks are given in section 7.

2. Security challenges

RFID is a pervasive system. Security of this system is equally important. An attacker can harm at various points including information eavesdropping at end

user sites, obstructing physical access, controlling the devices and stealing the information etc. Protection from these threats demands strong mechanism for confidentiality, integrity, authentication, availability and non-repudiation[31–35]. This protection mechanisms should addresses major security concerns in RFID system like [36, 37]:

- *Privacy:* No one is interested to reveal personnel information to others without being part of authentic process. This privacy leakage could bring up many frauds. For example, if some item is equipped with tag and store name, price, area and other item information then a robber can easily fetch the information that how much he can earn with one or more robberies in a particular area. Similarly, unauthentic reader can scan the information written on e-passport to locate the important persons or count the gathering in an area [38–40]. This could result in planning of some terrorist activities. Thus, privacy of personnel or correspondence information leakage through RFID system is a major concern.

- *Tracking:* Objects, persons, animals etc. tracking through RFID readers and tags increases the information vulnerabilities also. This information availability helps to create profiles and important information can be leaked from these profiles [41]. This information can be used in various unauthentic or uninterested activities like: advertisement, etc. For example, if customer is buying items from a shop on a regular interval and each item is equipped with RFID tag then customer profile can be created in a database. This profile helps to put similar interest customers in a group. An advertisement can be floated of special interests for these groups which may not be interest to customers. Equipments used to track items, people or animal attached with RFID tags are not expensive thus data collection for these advertisements, promotions or gathering future requirements to earn profits is much easier. As compared to other tracking techniques like: video surveillance, RFID system based technique is much cheaper and faster. Thus, it is beneficial to both authentic and unauthentic users. Hence, it demands strong security mechanism to protect the information at any stage of system. Protected information results in wide applications of RFID technology.

- *Eavesdropping:* This is one of the most common forms of attack in networks where there is use of radio frequency for data communication. An eavesdropper can deploy an antenna to collect the information transmitted between reader and tag. Tags and readers communicate at different frequency bands like: low, high, ultrahigh and microwave. Thus, distance and location of eavesdropper from reader or tag is important. An attacker eavesdrop information in reader to tag (forward eavesdropping), tag to reader (backward eavesdropping), operation zone of reader and randomly selected distance directions. Since, it is easily feasible to fetch the information at longer distance and without any difficulty hence this attack should be handled properly. In real time applications, if an attacker deploy antenna to eavesdrop the information then information from RFID systems like e-passports, payment systems, identity cards, tickers etc. is on stake [42–44]. This information could reveal personnel data.

- *Skimming:* Eavesdropping is intercepting the information during its transit whereas skimming is reading the information from its store stage. Like eavesdropping, skimming attack can fetch the information from real time

applications like: e-passports, identity cards, traveling tickers or passes, consumer products etc. This could again reveal the personnel information like: name, birth date, financial account details, photo etc. Anti-skimming devices designed to protect against this attack uses reverse electromagnetic field. Anti-skimming devices are lightweight, persistent and easy to carry.

- *Cloning:* Resource constraint RFID devices are easy to clone because high security classical primitives cannot be implemented on these devices. RFID passive devices are cost effective as it does not require battery source. These devices gain power from reader thus easy to clone. Similarly, cloning devices could be passive and gain power from reader. Passive cloning devices are put closer to original device. Passing a cloning device closer to original device and making a copy of the data for cloning purpose may just take few seconds or minutes. This could be more dangerous for those devices which do not provide strong protection like: employee ID cards, train or bus ticket passes, product vouchers in supply chain management etc. Several solutions have been proposed to protect tags from cloning. Authentication is one of them. In authentication based mechanism, a random number is generated and exchanged. Response to this random number exchange uses cryptography primitives like digital signature, hashing, encryption/decryption, message authentication code etc. Verification of this response is performed at other side. If response is verified then tag is considered to be authentic else unauthentic or cloned. A new random number is generated every time a tag is read. This process further protects the tags from cloning.

- *Replay attacks*: In RFID system, one reader scans multiple tags and one tag could be associated with multiple readers. Replay attacks occur when freshness and aliveness of messages are not handled properly. If traceability is not a major concern then random number or nonce help to stop replaying of messages. A sequence number synchronizes the information between tag and reader. Count of numbers generated is limited in fixed length sequence number. Thus, an attacker can play old sequence number in new session. In order to avoid replaying an old sequence number in new session, aliveness of message is important [4, 45–47]. A computational challenge aliveness of message along with freshness hinders the attacker to play a replay attack. This attack is common among ultra-lightweight protocols where bitwise logical operators are only allowed [46, 48]. These operators are easy to break because of least computational breaking challenge.

- *Relay attack:* In this type of attack, RFID tags and readers are mislead by providing false information. For example, if some reader is interested to scan a tag then attacker tag claims that it is the targeted tag [49]. Whereas, attacker tag fetches the information from another attacker reader which is close to authentic tag [50]. Thus, one reader and one tag attacker provide false information to authentic reader and tag [51, 52]. These authentic reader and tag are not in range of each other but attacker readers and tags mislead them to be close [53]. Attackers tries to prove the reader that the destination tag is nearby which is not in actual.

- *Denial of Service (DoS):* Radio signal blocks, active and passive jamming, packet overflows etc. are the signs of DoS attack. Low cost passive devices are resource constraint devices thus this attack easily blocks the services and it is more dangerous. An attacker floods the packets towards specific or set of

nodes. This results to blockage in services. Many solutions are proposed to observe this attack through graphs, behaviors, trusts, performance, quality of service etc. Detection of this attack is easier as compared to removal of attack in resource constraint networks [54].

- *Spoofing Attack:* This attack modifies the identity, address or naming services to provide false information. For example, an attacker claims to have certain IP address, MAC address or domain name which is not true. Here, attacker aims to eavesdrop or modify the information during its transit [55, 56].

- *Secret disclosure attacks:* In this attack, vulnerabilities of key updating, data centre processing, reader or tag computing etc. reveal the identity or key information [57]. This attack is common in ultra-lightweight authentication protocols where some secret information is known to adversary. Secret disclosure attack could result to other attacks like: de-synchronization, impersonation, eavesdropping etc. Since, algebraic computing is main cause of this attack thus it is dangerous for low cost passive RFID devices [58].

3. Authentication protocols, classifications and security issues

Recently developed RFID authentication protocols in classical, lightweight, ultra-lightweight and grouping proof protocols are discussed in this section. This section also discusses the latest attacks found on recently developed authentication protocols.

Authentication Protocols in Classical Cryptography Primitives Category.

This work discusses authentication protocols that uses classical cryptography [59]. Symmetric and asymmetric are two major types of classical cryptosystems. Protocols in these categories are as follows:

Symmetric Cryptography Primitives based Authentication Protocols.

Protocol (A1): Cheng et al. Protocol [60].

Premise: Let 'R', 'T' and 'DC' represent the reader, tag and data centre respectively. Let r_i, e_i and dc_i are the random numbers. Every tag selects its unique identification (ID) with its hash as H(ID). $K_{Session}^{Old}$ and $K_{Session}^{Current}$ are the old and current session key between R and T respectively. P(.) represents the enhanced chebyshev polynomial.

Step 1:- R ➔ T : r_1

Step 2:- T : $temp_1 = H(ID) \oplus e_1 \oplus r_1$

: $temp_2 = P_{r_1,e_1}\left(K_{Session}^{Current}\right)$

: $temp_3 = K_{Session}^{Current} \oplus e_1$

T ➔ R : $temp_1$, $temp_2$, $temp_3$

Step 3:- R ➔ DC : r_1, $temp_1$, $temp_2$, $temp_3$

Step 4:- DC : Computes $H(ID) \oplus K_{Session}^{Current} = temp_1 \oplus temp_3 \oplus r_1$

: $temp_4 = H(ID) \oplus K_{Session}^{Current}$

: if $temp_4$ record exist in data centre then fetch H(ID), $K_{Session}^{Current}$, $K_{Session}^{Old}$: $temp_5 = temp_1 \oplus H(ID) \oplus r_1$

: $temp_6 = H(ID) \oplus r_1 \oplus dc_1$

: if $temp_2$ equals to $P_{r_1}\left(P_{e_1}\left(K_{Session}^{Current}\right)\right)$ then

: $temp_7 = P_{dc_1,e_1}\left(K_{Session}^{Current}\right)$, $K_{Session}^{Old} = K_{Session}^{Current}$ and $K_{Session}^{Current} = K_{Session}^{Current} \oplus (e_1 || dc_1)$

: else if $temp_2$ equals to $P_{r_1}\left(P_{e_1}\left(K_{Session}^{Old}\right)\right)$ then
: $temp_7 = P_{dc_1,e_1}\left(K_{Session}^{Old}\right)$ and $K_{Session}^{Current} = K_{Session}^{Old} \oplus (dc_1 || e_1)$
: else tag is unauthentic
: Now, if tag is authentic then

DC ➔ R : $temp_6$, $temp_7$
Step 5:- R ➔ T : $temp_6$, $temp_7$
Step 6:- T : $dc_1 = temp_6 \oplus H(ID) \oplus r_1$
: if $temp_7$ equals to $P_{dc_1,e_1}\left(K_{Session}^{Current}\right)$ then $K_{Session}^{Current} = K_{Session}^{Current} \oplus (e_1 || dc_1)$

Explanation: Cheng et al. proposed random number and hash based authentication protocol in 2013 [60]. In this protocol, reader starts the authentication process. It selects a random number and sends it to tag (step 1). Tag computes three responses $temp_1$, $temp_2$ and $temp_3$ with the help of random numbers, H(ID), $K_{Session}^{Current}$ and P(.). Now, tag sends r_1 and three responses to reader (step 2). Reader forwards this information to datacentre (step3). Data centre verifies the tag entry record in database. Further, if tag is authentic then datacentre computes two responses for reader: $temp_6$ and $temp_7$ (step4). Reader forwards these responses to tag (step5). Tag verifies the authenticity of reader by comparing $temp_7$ with $P_{dc_1,e_1}\left(K_{Session}^{Current}\right)$. If both are equal then reader is considered to be authentic and symmetric session key is generated [36, 37, 46, 61, 62].

Protocol (A2): Single Entity-Single Communication based Unilateral Authentication Protocol.

Premise: Let 'R' and 'T' represents reader and tag respectively. Suppose, r_i and e_i are the i^{th} random numbers. A symmetric key 'K' is shared between reader and tag. $E_K(.)$ and $D_K(.)$ are the encryption and decryption functions [63].

Version 1:
Step 1:- R ➔ T : $E_K\{ID_T\}$
Step 2:- T : Verify $\{D_K\{ID_T\}\}$

Version 2:
Step 1:- T ➔ R : $E_K\{ID_T\}$
Step 2:- R : Verify $\{D_K\{ID_T\}\}$

Explanation: In single entity-single communication based unilateral authentication protocol, two variations of protocols are possible. In first variation, reader sends an encrypted identification based message to tag (step 1) and tag verify its identity (step 2). In second version, tag sends its encrypted entity to reader (step 1) and reader authenticates it by decryption and verification (step 2) [64].

Protocol (A3): Single Entity-Two Communications based Unilateral Authentication Protocol.

Premise: Let 'R' and 'T' represents reader and tag respectively. Suppose, r_i and e_i are the i^{th} random numbers selected by reader and tag respectively. A symmetric key 'K' is shared between reader and tag. $E_K(.)$ and $D_K(.)$ are the encryption and decryption functions.

Version 1:
Step 1:- R ➔ T : $\{r_1\}$
Step 2:- T ➔ R : $E_K\{r_1\}$
Step 3:- R : Verify $E_K\{r_1\}$

Version 2:
Step 1:- T ➔ R : $\{e_1\}$
Step 2:- R ➔ T : $E_K\{e_1\}$
Step 3:- T : Verify $E_K\{r_1\}$

Explanation: There are two version of single entity two communications based unilateral authentication protocol. In first version of protocol, reader initiates the authentication process by sending a random number challenge (step 1). Tag encrypts the received random number with symmetric key shared between tag and reader, and forwards it to reader (step 2). Now, reader re-encrypts its own random number challenge and verifies by comparing with the received data (step 3). If both are equal then tag is considered to be authentic. Similarly in second version, tag initiates the authentication process by sending a random number challenge (step 1). Reader encrypts the challenge with symmetric key and sends it to tag (step 2). Tag verifies the response for authentication (step 3) [65].

Asymmetric Cryptography Primitives based Authentication Protocols.

Like symmetric cryptography, asymmetric cryptography primitives based protocols are also designed to enhance the security of system. Major of recently developed asymmetric protocols are based on elliptic curve cryptography. This section discusses the recently developed elliptic curve cryptography based authentication protocols. Recently analyzed attacks on some of the authentication protocols are also explored.

Elliptic Curve Cryptography (ECC) based Authentication Protocols.

Protocol (B1): Authentication mechanism with ECC Encryption/Decryption for end users.

Premise: Let 'R' and 'T' represents reader and tag respectively. Suppose, r_i is the i^{th} random number selected by reader or tag. Let C_j and P_j represent the ciphertext and plaintext generated at i^{th} side. Where, $j \epsilon \{R, T\}$. Encryption and decryption functions at j^{th} side are represented by $E_j()$ and $D_j()$. Unique identification of tag and reader is represented by ID_T and ID_R respectively. Let 'h' is the hash function used to generate the digest.

Step 1:- R : Selects 'r_1' ϵZ_n
: Calculate (i) $H = h(r_1)$
(ii) $C_R = E(r_1, ID_T)$
R ➔ T : C_R, ID_T, H
Step 2:- T : $(y, ID_T) = D(C_R)$
: Verify [h(y)==H] and [decrypted ID_T]
T ➔ R : y
Step 3:- R : if y== r_1 then 'T' is authentic else unauthentic.

Explanation: This is random number generation based authentication protocol. Here, reader selects a random number and computes the ciphertext of tag identification with this random number. Reader sends the ciphertext, tag identification and hashing over random number to tag (step 1). After receiving the data, tag decrypt the encrypted information and fetches the random value and tag identification. Here, tag verifies the received hash value with regenerated hash value. If both are verified then tag sends the decrypted random number value to reader (step 2). Reader verifies the received random value with its own generated random value in step 1. If it matches then user associated with tag is considered to be authentic otherwise unauthentic (step 3). This protocol was developed by taking consideration that protocol is protected from replay, reflection and chosen-text attacks due

to encryption/decryption and hash functions. Use of encryption/decryption and hash functions is the major cause that this protocol is not suitable for resource constraint devices.

Protocol (B2): ECC based signature-based mechanism for authenticating end users.

Premise: - Let 'R' and 'T' represents reader and tag respectively. Suppose, r_i and e_i are the i^{th} random number selected by reader and tag respectively, ID_r represents the identification of reader, $CERT_{TAG}$ represents the certificate pre-shared between tag and reader, and SIGN and VERIFY represents the digital signature based signing and verification processes.

Step 1:- R ➔ T : r_1
Step 2:- T : $y = SIGN(r_1, r_2, ID_r)$
T ➔ R : r_2, ID_r, y, $CERT_{TAG}$
Step 3:- R : VERIFY $CERT_{TAG}$ and VERIFY y
: if verified then consider that tag is valid.

Explanation: Reader starts the authentication process by sending a random challenge to tag (step 1). Tag selects another challenge and digitally signs both challenges along with the identification of reader. This signature message, random challenge, identification of reader and tag's certification is sent towards tag (step 2). Now, reader verifies both the certificate and digital signature. If both are verified then tag is considered to be authentic else unauthentic (step 3). Author claims that this protocol prevents existential forgery attack.

Protocol (B3): Schnorr Identification scheme and end-user verification with ECC [55].

Premises:-
Let 'R' and 'T' represents reader and tag respectively. Suppose, r_i and e_i are the i^{th} random number selected by reader and tag respectively. Tag's public key is represented by Z and P is the base point selected on elliptic curve E.

Step 1:- T : Computer $X = r_1P$
T ➔ R : X
Step 2:- R ➔ T : e_1
Step 3:- T : Compute $y = ae_1 + r_1$
T ➔ R : y
Step 4:-R : if $yP + e_1Z == X$ then authentic else unauthentic

Explanation: Tuyls proposed schnorr identification protocol based on elliptic curve discrete logarithmic problem in 2006. In this protocol, tag starts the communication by sending $X = r_1P$ to reader (step 1). Reader receiver the message X. To verify this message and tag, it sends a random number to tag (step 2). Now, tag responds with 'y' to the reader (step 3). Reader verifies the message 'X' with the help of tag's public key. If it matches then tag is considered to be authentic else unauthentic. In this protocol, an attacker reader can easily trace the tag by acting as a middle entry between tag and reader. Attacker reader function is explained in attack 1.

Attack 1: Tag tracing by attacker reader on ECC and Schnorr Identification scheme.

Premises: In addition to premises of protocol, let $R_{attacker}$ is the eavesdropper that want to trace the tag.

Step 1:- T ➔ $R_{attacker}$: X
Step 2:- $R_{attacker}$ ➔ R : X'

Step 3:- $R \rightarrow R_{attacker}$: e_1
Step 4:- $R_{attacker} \rightarrow T$: e_1
Step 5:- $T \rightarrow R_{attacker}$: $y = ae_1 + r$
: Now, $R_{attacker}$ is knowing X, e_1 and $y = ae_1 + r$.
Step 6:- $T \rightarrow R_{attacker}$: X''
Step 7:- $R_{attacker} \rightarrow T$: $e_2(=e_1)$
Step 8:- $T \rightarrow R_{attacker}$: $y' = ae_2 + r'$
: computes $y'P + e_2Z = X'$

Explanation: Now, attacker reader can easily trace the tag by checking whether $(y'-y)P$ equals $(X'-X)$. In this attack, $R_{attacker}$ communicates with 'T' and 'R' to trace 'T'. Here, 'T' communicates with $R_{attacker}$ instead of 'R' (step 1). $R_{attacker}$ does not generate a challenge by itself but forwards the e_1 received from 'R' to 'T' (step 2 to step 4). In continuation, 'T' responses to challenge but it go to $R_{attacker}$ instead of 'R'(step 5). Later, 'T' communicates again with $R_{attacker}$. 'T' and '$R_{attacker}$' again generate new challenges and responses (step 6 and step 8). Now, $R_{attacker}$ can keep trace of the 'T' by computing whether $(y'-y)P$ equals $(X'-X)$.

Attack 2: If attacker reader knows the public key 'Z' of tag then it can easily compute the message by computing $yP + e_1Z = X$. Thus, this mechanism is not considered to be secure against forward secrecy.

In addition to attack 1 and attack 2, this protocol is having scalability issues. Cost of computation at reader side is high since increase in number of tags handled per reader requires most of the public keys to be accessed from database by the reader. This increases the computational cost of reader. Increase in computational cost reduces the power of reader to handle more tag. Thus, scalability of network reduces gradually.

4. Lightweight authentication protocols

Lightweight authentication protocols are less powerful as compared to classical cryptography based protocols. Lightweight cryptography is integrated with protocols to achieve confidentiality, integrity, availability, authentication and non-repudiation. Apart from security, communication and computational cost at reader and tag is another factor taken into consideration for selecting the lightweight authentication protocol.

Protocol (C1):-
Yu et al. Protocol [49].

Premises:-
Let 'R' and 'T' represents reader and tag respectively. Suppose, r_i and e_i are the i^{th} random number selected by reader and tag respectively. Let 'm' represents the m-bit map in form of non-volatile memory. This non-volatile memory is used to store random number information to protect from tracking attack.

Step 1:-$R \rightarrow T$: r_1
Step 2:-T : Compute $j = h(k_i, r_1) \bmod m$
: if map[j] is zero then
: map[j] = 1 and
$T \rightarrow R$: $h(k_i, r_1)$
: else if map[j] is non-zero then
$T \rightarrow R$: $h(k_i, e_1)$
Step 3:- $R \rightarrow DC$: $h(k_i, r_1)$ or $h(k_i, e_1)$.

Step 4:- DC : find entry for $h(k_i, r_1)$ or $h(k_i,e_1)$ in database. If entry found then
: Compute $h(k_i + 1, r_1)$ or $h(k_i + 1,e_1)$
: Update k_i with $h(k_i)$ and hash value with $h(k_i, r_2)$
DC ➔ R : $h(k_i + 1, r_1)$ or $h(k_i + 1,e_1)$
: if entry does not found in database then
DC ➔ R : DENY
Step 5:- R : if response from DC is DENY then
R ➔ T : r_3
: else
R ➔ T : $h(k_i + 1, r_1)$ or $h(k_i + 1,e_1)$
Step 6:- T : Compute $h(k_i + 1, r_1)$ or $h(k_i + 1,e_1)$ again
: Compare received message with computed message. If they are equal then
: Update its key with $h(k_i)$ and all bits of map equals to zero.

Explanation: This is a random number based authentication protocol. Reader starts a process of authentication by selecting a random number and sending towards tag (step 1). Tag computes its position and search the corresponding bit position on map. If bit position is zero on map then it sends its position to reader else selects a new random number and send towards tag (step 2). Reader sends the received value to data centre (step 3). Data centre searches the record in database. If entry found in database then it updates key and hash values. Updated information is forwarded to reader (step 4). If entry is not found in database then a DENY message is replied. Reader checks the received message. If received message is not DENY message then it forwards the received message to tag (step 5). Now, tag re-computes the hash value. If new hash value is equal to received value then tag also updates its hash value. It sets all bits of map to zero (step 6).

Protocol (C2):-
Mitra et al. protocol [51].

Premises:-
Let 'R' and 'T' represents reader and tag respectively. Suppose, r_i and e_i are the i^{th} random number selected by reader and tag respectively.

Step 1:- R ➔ T_i :{request}
Step 2:- T : Compute $IDS = e_1*K + ID_T$
T ➔ R : IDS
Step 3:- R : ID'_T=IDS mod K

Explanation: Mitra proposed authentication protocol to protect against traceability and cloning in 2008 [51]. Reader to tag or tag to reader eavesdropping in communication is feasible in this protocol. In this protocol, reader starts the process by sending a random number (step 1). Tag computes the identification pseudonym and sends it to reader (step 2). Reader extracts the identification from received data (step 3).

Attack:- Cloning attack on Mitra Protocol.
Step 1:- R ➔ T : {request}
Step 2:- T : Compute $IDS_1 = e_1*K_1 + ID_T$
T ➔ $R_{Attacker}$: IDS_1
Step 3:- $R_{Attacker}$ ➔ R : IDS_1
Step 4:- R : ID'_T=IDS_1 mod K_1

R ➔ T : {request}
Step 5:- T ➔ $R_{Attacker}$: $IDS_2 = e_2 * K_2 + ID_T$
Step 6:- $R_{Attacker}$ ➔ R : IDS_2
...
...
Step n-2:- T ➔ $R_{Attacker}$: $IDS_n = e_n * K_n + ID_n$
Step n-1:- $R_{Attacker}$ ➔ R : IDS_n
Step n: - R : $ID'_T = IDS_n \bmod K_n$
Step n + 1:- $R_{Attacker}$: Collects $IDS_1, IDS_2, ..., IDS_n$.
: Compute $temp_1 = (IDS_2-IDS_1)*K_1$, $temp_2 = (IDS_3-IDS_2)*K_2$, ..., $temp_{n-1} = (IDS_n-IDS_{n-1})*K_{n-1}$.
: Compute $K_i = GCD(temp_1, temp_2, ...temp_{n-1})$

Explanation: In this attack, an attacker observes the communication between tag and reader [52]. Attacker observes and record IDS_1 to /IDS_n values (step 2, step 5, step n-2). This attacker again calculates $temp_1$ to $temp_{n-1}$ values and greatest common divisor (GCD) of these values (step n + 1). This GCD value is the secret key of tag in communication. Here, an attacker can start the message exchange with tag by collecting $temp_i$ and sending $IDS_i + r_i*temp_i$ to tag. This is an easy way to clone.

Attack:- Traceability attack in Mitra's protocol.
Step 1:- $R_{Attacker}$ ➔ T : {request}
Step 2:- T ➔ $R_{Attacker}$: IDS_1
...
...
Step i:- $R_{Attacker}$ ➔ T : {request}
Step i + 1:- T ➔ $R_{Attacker}$: IDS_i
Step i + 2:- $R_{Attacker}$ ➔ T : {request}
$R_{Attacker}$ ➔ T' : {request}
Step i + 3:- T ➔ $R_{Attacker}$: IDS_n
Step i + 4:- T' ➔ $R_{Attacker}$: IDS_{n+1}
Step i + 5:- $R_{Attacker}$: accept IDS_n if b==0, accept IDS_{n+1} if b==1
: Compute $temp_1 = IDS_1-IDS_i$
: Compute $temp_2 = \begin{cases} IDS_1 - IDS_n \; if \; b == 0 \\ IDS_n - IDS_{n+1} if \; b == 1 \end{cases}$
: Select $\begin{cases} d = 0 \; if \; GCD(temp_1, temp_2) \geq 2^{L/2} \\ d = 1 \; if \; GCD(temp_1, temp_2) < 2^{L/2} \end{cases}$

Explanation: Traceability attack in this protocol start with two requests from reader to tag (step 1 to step i + 1). In response to these requests, tag receives encrypted messages: IDS_1 and IDS_i. Attacker again sends two requests to associated identifications (ID_T, ID'_T) based tags (step i + 2). These tags return encrypted messages: IDS_n and IDS_{n+1} (step i + 3 and i + 4). Attacker accepts these messages from different tags in different form. It accepts IDS_n and IDS_{n+1} from tags with identification ID_T and ID'_T respectively. It uses b = 0 for ID_T and b = 1 for ID'_T to distinguish between tags and further necessary computations. Attacker computes $temp_1$ and $temp_2$ from received encrypted messages (step 5). Now, attacker guesses the bit based on length decision rule. Peris-Lopez found a success probability of guessing equal to 1 and this result in traceability with 50% probability [52].

Attack:- Full disclosure attack on Mitra's protocol

Explanation: As seen in cloning attack, attacker observes the messages exchange between tags and reader. This results in obtaining the secret key of tag with the help of GCD computations. After getting the secret of tag, attacker can easily reveal the stored and transmitted information. Peris-Lopez calculated the probability of revealing the secret using Riemann zeta function [52]. Authors found a success rate of 60 to 100% of this attack and claim that it is most dangerous among all discussed attacks.

Protocol (C3): Qingling et al.'s protocol [51]

Premises: Let 'R', 'T' and 'DC' represents the reader, tag and data centre respectively. Suppose r_i, e_i and dc_i are the random numbers selected by reader, tag and data centre respectively. MSB and LSB represents the most and least significant bits of a unique identifier (UID^T) and access password ($PASSWD^T$).

Step 1:- R ➔ T_i : r_i

Step 2:- T_i : $Message^{T_i} = Message^{T_i}_{LSB} || Message^{T_i}_{MSB}$

: $Message^{T_i}_{LSB} = \text{CRC}(UID^{T_i}_{LSB} \oplus r_i \oplus e_i) \oplus PASSWD^{T_i}_{LSB}$

: $Message^{T_i}_{MSB} = \text{CRC}(UID^{T_i}_{MSB} \oplus r_i \oplus e_i) \oplus PASSWD^{T_i}_{MSB}$

T_i ➔ R : $\{Message^{T_i}, e_i^{T_i}\}$

Step 3:- R : Verify $Message^{T_i} \oplus PASSWD^{T_i}$ equals to CRC $(UID^{T_i}_{LSB} \oplus r_i \oplus e_i)$ || CRC$(UID^{T_i}_{MSB} \oplus r_i \oplus e_i)$. If this condition holds for any tag in data centre then tag is authentic and process continues else unauthentic.

: Compute $\text{Message}^R = Message^R_{LSB} || Message^R_{MSB}$, Where, $Message^R_{LSB} = \text{CRC}(UID^{T_i}_{LSB} \oplus r_i^{T_i}) \oplus PASSWD^{T_i}_{LSB}$ and $Message^R_{MSB} = \text{CRC}(UID^{T_i}_{MSB} \oplus r_i^{T_i}) \oplus PASSWD^{T_i}_{MSB}$.

R ➔ T_i : Message^R

Step 4:- T : Verify $\text{Message}^R \oplus PASSWD^{T_i}$ equals to $\text{CRC}(UID^{T_i}_{LSB} \oplus r_i^{T_i})$ || $\text{CRC}(UID^{T_i}_{MSB} \oplus r_i^{T_i})$. If condition holds then reader is authentic else unauthentic.

Explanation: Qingling et al. [66] proposed a lightweight authentication protocol based on password challenge [51]. Reader starts the authentication process by sending a random number challenge to tag (step 1). Tag constructs most significant and least significant part of message to generate response for reader. Most significant and least significant parts are XORed with passwords before sending it to reader (step 2). Reader verifies the received messages and generates new challenge for tag to prove its authenticity (step 3). Tag verifies the received message for reader authenticity (step 4).

Attack:- Attack on Qingling et al.'s protocol.

Premise:- An attacker eavesdrops one session between 'R' and 'T'.

Step 1:- $R_{Attacker}$ ➔ T_i : $Message^{T_i}_{LSB} \oplus \text{CRC}(\alpha) || Message^{T_i}_{MSB} \oplus \text{CRC}(\alpha), e_i^{new}$. Where, $\alpha = \delta + \gamma$. $\delta = e_i^{new} \oplus e_i$, $\gamma = r_i^{new} \oplus r_i$.

Step 2:- $R_{Attacker}$ ➔ R : $Message^R_{LSB} \oplus \text{CRC}(\delta) || Message^{T_i}_{MSB} \oplus \text{CRC}(\delta)$. Where, $\delta = e_i^{new} \oplus e_i$.

Explanation: Peris-Lopez et al. discovered impersonation of tag and reader in two communications [52]. This is possible by passively observing the one session between tag and reader. This impersonation helps the attacker to send a message with new random values (e_i^{new} and r_i^{new}). Now, verification of this message at tag

side is easy (step 1). Similarly, an attacker can supplant the reader with a message containing new random variables (e_i^{new}). This message authenticates the attacker as a genuine reader. Tag can not detect this attack easily (step 2).

Attack:- Traceability attack on Qingling et al. protocol.
Step 1 (Learning):

$R_{Attacer}$: Acquire r_1, e_1 and $Message^{T_0} = Message_{LSB}^{T_0}||$ $Message_{MSB}^{T_0}$, $Message_{LSB}^{T_0} = CRC(UID_{LSB}^{T_0} \oplus r_1 \oplus e_1) \oplus PASSWD_{LSB}^{T_0}$, $Message_{MSB}^{T_0} = CRC(UID_{MSB}^{T_0} \oplus r_1 \oplus e_1) \oplus PASSWD_{MSB}^{T_0}$.

Step 2 (Challenge):

$R_{Attacer}$: Selects two tags with UID^{T_0} and UID^{T_1}. It execute a test query that result to return two random numbers r_1^{new} and $e_2^{T_i}$, and message $Message^{T_i} \in \{Message^{T_0}, Message^{T_1}\}$. Selection of message is dependent on random bit $b \in \{0,1\}$. $\{CRC\left(UID_{LSB}^{T_0} \oplus r_1^{new} \oplus e_2^{T_0}\right) PASSWD_{LSB}^{T_0}||$ $CRC(UID_{MSB}^{T_0} \oplus r_1^{new} \oplus e_2^{T_0}) \oplus PASSWD_{MSB}^{T_0}$ if {b==0}or $\{CRC\left(UID_{LSB}^{T_0} \oplus r_1^{new} \oplus e_2^{T_1}\right) PASSWD_{LSB}^{T_1}||$ $CRC(UID_{MSB}^{T_1} \oplus r_1^{new} \oplus e_2^{T_1}) \oplus PASSWD_{MSB}^{T_1}$ if b==1}

Step 3 (Guessing):

$R_{Attacer}$ **:** An attacker obtains constant 1 and constant 2 values from step 1 and step 2 respectively. These values are associated to T_0. $Constant1_{LSB} = Message_{LSB}^{T_0} \oplus CRC(r_1) \oplus CRC(e_1) = CRC(UID_{LSB}^{T_0}) \oplus PASSWD_{LSB}^{T_0}$. $Constant1_{MSB} = Message_{LSB}^{T_0} \oplus CRC(r_1) \oplus CRC(e_1) = CRC(UID_{MSB}^{T_0}) \oplus PASSWD_{MSB}^{T_0}$. $Constant1 = Constant1_{LSB}||Constant1_{MSB}$. $\{CRC\left(UID_{LSB}^{T_0}\right) \oplus PASSWD_{LSB}^{T_0}||$ $CRC(UID_{MSB}^{T_0}) \oplus PASSWD_{MSB}^{T_0}$ if {b==0}or $\{CRC\left(UID_{LSB}^{T_0}\right) \oplus PASSWD_{LSB}^{T_1}||$ $CRC(UID_{MSB}^{T_1} \oplus PASSWD_{MSB}^{T_1}$ if b==1. An attacker calculate value of output bit d = {0 if constant1 equals to constant2, 1 if constant 1 not equals to constant 2}.

Explanation: Peris-Lopex et al. calculated the probability to distinguish between tags in order to interact for traceability [52]. This probability is high because it is easy to distinguish between tags. Thus, it is easy to implement traceability attack with above sequence of steps. There are three stage of observation: learning, challenge and guessing. Learning state observe the transactions between reader and tag to collect the secret parameters. Challenge step put random number based challenges to tag through attacker. Finally guessing state finds the probability of receiving 0 or 1.

Protocol (C4): LRAP (Lightweight RFID Authentication protocol) [67]

Premises:- Let 'R', 'T' and 'DC' represents the reader, tag and data centre respectively. Suppose r_i, e_i and dc_i are the random numbers selected by reader, tag and data centre respectively. Further, IDS, C_i, K_E, K_D are the identification pseudonym, i^{th} ciphertext, encryption and decryption keys respectively.

Step 1:- R ➔ T : {Hello}
Step 2:- T ➔ R : {IDS}

Step 3:- R : Compute ciphertext, $(C_1, C_2, C_3) = E_{K_E}(r_1, r_2)$, $C_3 = r_3P$, $(temp_1, temp_2) = r_3K_E$, $C_1 = temp_1 . r_1 \bmod N$, $C_2 = temp_2 . r_2 \bmod N$, $temp_3 = (IDS + r_1 + r_2) \oplus K_E$.

R ➔ T : $(C_1, C_2, C_3) \| temp_3$

Step 4:- T : Extract (r_1, r_2) from (C_1, C_2, C_3), $(temp_1, temp_2) = K_D.C_3$, $r_1 = C_1. temp_1^{-1} \bmod N$, $r_2 = C_2. temp_2^{-1} \bmod N$, Compute $temp'_3 = (IDS + r_1 + r_2) \oplus K_DP$ and verifies whether $temp'_3$ equals to $temp_3$. If both are equal then compute $temp_4 = (r_1 \oplus r_2) + ID$.

T ➔ R : $temp_4$

: Updation $IDS^{old} = IDS$, $IDS^{new} = (IDS^{old} + r_1) + (ID + r_2)$

Step 5:- R : Computes $temp'_4 = (r_1 \oplus r_2) + ID$, Verifies $temp'_4$ equals to $temp_4$. If both are equal then tag is authentic else unauthentic.

: Updation $IDS = (IDS + r_1) \oplus (ID + r_2)$.

Explanation: LRAP is elliptic curve based lightweight authentication protocol proposed by Liu et al. in 2013 [67]. Reader starts the authentication process by sending a hello request (step 1). Tag responds with its identification pseudonym (step 2). Reader response to tag includes the ciphertexts append with identification pseudonym (step 3). These ciphertexts are generated by encrypting the reader generated random numbers with encryption key. After receiving the response from reader, tag extracts the random numbers and verifies it. If these are verified then compute a new identification and random number based response to reader (step 4). After this communication, tag initiates the identification pseudonym updating process. On receiving the response, reader verifies it for authenticity and initiated the identification pseudonym updating process (step 5).

5. Grouping/yoking authentication protocols

This section discusses the protocols that allows the multiple tags to authentication simultaneously with same reader. Multiple tag authentication constructs groups with unique group identifications. Group construction is possible through collaborations of tag to jointly request the reader for authentication. Following are the important group authentication protocols [68].

Protocol (E1): Juels Yoking Protocol [69, 70].

Premise:- Let 'R', 'T' and 'DC' represents the reader, tag and data centre respectively. Let r_i and e_i are the random number selected by reader and tag respectively. Suppose, 'K_i' is the shared key between reader and i^{th} tag, MAC is the message authentication code.

Step 1:- R ➔ T_1 : {hello}

Step 2:- T_1 ➔ R : ID_{T_1}, e_1

Step 3:- R ➔ T_2 : e_1

Step 4:- T_2 ➔ R : ID_{T_2}, e_2, $temp_1 = MAC_{K_2}[e_1]$

Step 5:- R ➔ T_1 : e_2

Step 6:- T_1 ➔ R : $temp_2 = MAC_{K_1}[e_2]$

Step 7:- R ➔ DC : $\{ID_{T_1}, e_1, temp_2, ID_{T_2}, e_2, temp_1\}$

Explanation: Juel's grouping protocol is the first group authentication protocol [71, 72]. This is the simplest protocol to understand and implement. Reader starts

the authentication process by sending a random number based challenge (step 1). Tag responds with its identification mark and another random number challenge (step 2).

Protocol (E2): Saito and Sakurai's Protocol [73].

Premise:- Let 'R', 'T' and 'DC' represents the reader, tag and data centre respectively. Suppose, 'K_i' is the shared key between reader and i^{th} tag, MAC is the message authentication code. PT is the pallet tag.

Step 1:- DC ➔ R : {timestamp}
Step 2:- R ➔ T_i : {timestamp}, Where $i \in \{1,n\}$
Step 3:- T_i ➔ R : $temp_i = MAC_{K_i}$[timestamp]
Step 4:- R ➔ PT : {timestamp}, $temp_i$,
Step 5:- PT ➔ R : E_K[{timestamp}, $temp_i$]
Step 6:- R ➔ DC : {timestamp, E_K[{timestamp}, $temp_i$], ID_{T_1}}

Explanation: Saito and Sakurai protocol tried to remove replay attack from juel's protocol [74]. Data centre initiated the group authentication proof protocol by sending a timestamp message to reader (step 1). Reader forwards the timestamp to all tags (step 2). All tags then send a message authentication code of timestamp to reader (step 3). There is use of pallet tag in this protocol. This tag is assumed to have abundance of resources as compared to any existing tag. Reader forwards the timestamp message and message authentication code of all tags to pallet tag (step 4). Pallet tag encrypts the received message and sends it to reader (step 5). Reader forwards this message to data centre for storage (step 6). This stored entry is a grouping proof.

Attack: Secret disclosure attack on Kazahaya.

Explanation: Bagheri et al. found that it is possible for an attacker to retrieve tag's secret parameters at cost of $O(2^{16})$ offline random number evaluations [75]. In this attack, an attacker eavesdrops one session between tag and reader. Further, at cost of $O(2^{16})$ operations, it fetches private key of tag, identification of tag and group identification. These secret disclosure parameters increase the chance of tag and reader impersonation, and traceability. An attack can forge proofs at any time. It is found that verification of forged proofs is possible at cost of one session eavesdropping. Thus, forgery attack is another threat to this protocol and probability of this attack is '1'.

6. Comparisons

Security and cost analysis of authentication protocols is presented in this section. Security analysis is performed based on parameters selected in Section 3. Similarly, cost estimation is analyzed through communication and computational cost parameters. This analysis is performed to find authentication protocol suitable for resource constraint or resourceful devices in IoT.

6.1 Security analysis

Possibilities of attacks on surveyed authentication protocols are analyzed in security analysis. This comparison of authentication protocols is made through infeasible, strong, medium and weak possibilities of attacks. Authentication protocol attacks and their chance on studied protocols are searched from literature. If a direct attack is found then possibility of attack is considered to be strong (S).

Otherwise, attacker's dependency on existing attack is searched. For example, man-in-the-middle and denial of service attacks lead to de-synchronization and traceability attacks. Hence, if chances of man-in-the-middle and denial of service attacks is strong then de-synchronization and traceability attacks provide medium (M) chances. Similarly, eavesdropping leads to secret disclosure attack. Chances of indirect attacks are considered to be medium because extra computational and communication cost is required to perform these attacks. Further, chances of indirect attacks with high computational and communication cost are considered to be weak (W). Overall, it is analyzed that the recent trends is to design authentication protocols based on asymmetric key based cryptosystem because such protocol provide high security and low communicational cost as compared to symmetric key cryptosystem based protocols. Symmetric or asymmetric cryptosystem based authentication protocols are suitable for resourceful devices such as active RFID devices. These devices can afford the computational cost of protocols. Lightweight and ultra-lightweight protocols are designed for resource constraint devices like: passive RFID devices. These devices cannot afford high computations or storage. Security of such protocols is a major concern. It is impossible to fully secure such protocols from attacks. Protocol with higher attack resistant probability is considered to be more reliable. Hence protocol like C4, D2 and D3 are more reliable. Further, these authentication protocols can be extended to create groups called grouping or yoking protocols.

6.2 Cost analysis

Communication and computational cost of studied authentication protocols is analyzed in **Table 1**. Communication cost is measured in terms of number of transactions made between reader and tag. Different levels to measure the cost are Low (L), Medium (M) and High (H). If number of transactions is between 1 and 3 then communication cost is considered to be low. If it varies from 4 to 6 then communication cost is medium. Communication cost is considered to be high if number of transactions is more than 6. It is found that communication cost of asymmetric

Possibility of Attacks on Authentication Protocols															**Cost Analysis**	
Protocol	**P_r**	**T_r**	**FS**	**BS**	**E_a**	**S_k**	**C_l**	**R_P**	**R_L**	**DoS**	**S_P**	**S_D**	**D_E**	**M_M**	**C_{comm}**	**C_{omp}**
Symmetric Cryptography Primitives Based Authentication Protocols																
A1 [60]	S	M	M	M	M	M	M	W	M	M	M	S	S	S	M	H
A2	M	S	S	M	M	M	M	S	S	S	M	M	S	M	L	H
A3	S	S	S	M	S	M	M	S	S	S	S	S	S	S	L	H
Asymmetric Cryptography Primitives Based Authentication Protocols																
B1	S	S	S	M	W	M	M	M	M	M	M	M	M	M	L	H
B2	S	S	S	M	W	M	M	M	M	M	M	M	M	M	L	H
B3	S	S	S	M	W	M	S	S	S	S	S	S	S	S	L	M
Lightweight Authentication Protocols																
C1	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	H
C2 [51]	M	S	M	M	M	M	S	M	M	M	M	S	S	S	L	L
C3 [51]	M	S	M	M	S	M	M	M	M	M	S	M	S	S	L	L
C4 [67]	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	L

	Possibility of Attacks on Authentication Protocols														Cost Analysis	
Protocol	**P_r**	**T_r**	**FS**	**BS**	**E_a**	**S_k**	**C_l**	**R_P**	**R_L**	**DoS**	**S_P**	**S_D**	**D_E**	**M_M**	**C_{omm}**	**C_{omp}**
Ultra-lightweight Authentication Protocols																
D1 [36]	S	S	S	S	S	S	S	S	S	S	S	S	S	S	M	L
D2 [76]	M	S	M	M	M	M	M	M	M	M	M	M	S	M	L	H
D3 [77]	M	M	M	M	M	M	M	M	M	M	M	M	M	M	H	L
Group Authentication Protocols																
E1 ([71]; [72])	W	W	M	M	W	W	W	W	W	W	W	W	W	W	H	L
E2 [74]	W	W	M	M	W	W	W	W	W	W	W	W	W	W	M	L
E3 [37]	M	M	W	W	M	W	W	M	W	W	M	W	M	M	M	L

P_r = Privacy, T_r = Tracking, FS = Forward Secrecy, BS = Backward Secrecy, E_a = Eavesdropping, S_k = Skimming, C_l = Cloning, R_P = Replay, R_L = Relay, DoS = Denial of Service, S_P = Spoofing, S_D = Secret Disclosure. D_E = De-synchronization, M_M = Man-in-the-middle, W = Weak, M = Medium, S = Strong, C_{omm} = Communication Cost, C_{omp} = Computational Cost, L = Low, H = High.

Table 1.
Security and cost analysis of authentication protocols.

cryptography primitives based authentication protocols is much lower than any other type of authentication protocols. Although lightweight and ultra-lightweight protocols claim to be efficient for resource constraint devices but asymmetric cryptography based protocols can also be designed to reduce the overhead through reduction in communication cost. For example, protocol C4 is based on elliptic curve cryptosystem based asymmetric cryptography and it is efficient than any other lightweight protocol. Like communication cost, computational cost is also divided into three levels: Low, Medium and High. A high cost authentication protocol includes encryption, decryption, hashing or high computational functions. Medium cost based protocols include mathematical functions like elliptic curve based addition, multiplication or inverse, shift or permutation operations etc. A low cost protocol affords simple mathematical functions like: logical operations (AND, OR, NOT etc.), simple permutation, rotation random number generator etc. Lightweight and ultra-lightweight protocols are especially designed to count these low computational cost factors into considerations. Computational cost of these protocols is much lower than any classical cryptography based symmetric or asymmetric authentication protocols.

7. Conclusion

In this work, RFID authentication protocols from different categories are studied and compared on security requirements and cost. Authentication protocols are categorized as: symmetric, asymmetric, lightweight, ultra-lightweight and group based authentication based protocols. It is found that asymmetric cryptography based protocols are gaining popularity day-by-day and provide enough security. Symmetric and asymmetric cryptography based authentication protocols are suitable for resourceful devices. Passive RFID devices are resource constraint devices thus lightweight or ultra-lightweight protocols are more suitable. Security in lightweight protocols is a major challenge. Hardware limitations restrict the

implementation of full security on these devices. Thus, these devices can not be fully protected. Integration of asymmetric key cryptography based lightweight authentication protocols is contemporary topic of research. These unilateral or mutual authentication protocols can be extended for group authentication. Multiple tags authenticate itself with reader and store group information in data centre. This concept of group authentication is important for IoT. Authenticated devices in IoT increase the chances of secure communication in a network. Future work demands to construct a secure grouping proof protocol that is not affected with relay, replay or de-synchronization attacks.

Key terms and definitions

Active attacks	an illegal act of modifying the information or operation to affect the system
Asymmetric key cryptography	a cryptosystem that uses public and private keys for encryption and decryption process is known as asymmetric key cryptosystem
Authentication	a process to confirm the attributes of message/user is known as message or user authentication
Lightweight cryptography	a least computational cost based cryptosystem designed to provide security for resource constraint devices
Passive attacks	an illegal use of using the important system information using affecting the resources
Symmetric key cryptography	a cryptosystem that uses same or symmetric key for encryption and decryption operation
Yoking protocol	a group of participants authenticates each other for constructing a secure environment

Author details

Adarsh Kumar[1*] and Deepak Kumar Sharma[2]

1 Department of Systemics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India

2 Department of Informatics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India

*Address all correspondence to: adarsh.kumar@ddn.upes.ac.in

References

[1] Ashton, K. (2009). That 'Internet of Things' Thing, in the real world things matter more than ideas, *RFID Journal*, Retrieved July 15, 2014, from http://www.rfidjournal.com/articles/view?4986

[2] Uckelman D., Harrison M. and Michahelles F. (2011) Architecturing the Internet of Things. Springer-Verlag Berlin Heidelberg.

[3] Aggarwal, C. C., Ashish, N. and Sheth, A. (2013). The Internet of Things: A Survey from the data-centric Perspective. In Aggarwal, C (Ed.), *Managing and Mining Sensor Data* (pp. 383–428). Springer-Verlag.

[4] Abyaneh, M. R. S. (2012). Security Analysis of Lightweight Schemes for RFID Systems. Ph. D.Thesis, University of Bergen, Norway.

[5] Juel A. and Weis S. (2005). Authenticating Pervasive Devices with Human Protocols. In V. Shoup, editor, *Advances in cryptology-Crypto 05*, LNCS 3126, pp. 293–298, Springer-Verlag.

[6] Peris-Lopez, P., Hernandez-Castro, J. C., Esteveze-Tapiador, J. M. and Ribagorda, A. (2006). RFID Systems: A Survey on Security Threats and Proposed Solutions, *International Conference on Personal Wireless Communication- PWCA'06*, LNCS 4217, pp. 159–170, Albacete, Spain.

[7] Moore, G. E. (1965), Cramming More Components onto Integrated Circuits. Electronics: http://www.intel.com, (1965).

[8] Lopez, P. P. (2008). Lightweight Cryptography in Radio Frequency Identification (RFID) Systems, Ph. D. THESIS, UNIVERSIDAD CARLOS III DE MADRID. Madrid, Spain.

[9] Oren, Y. and Feldhofer, M. (2009). A Low-Resource Public-Key Identification Scheme for RFID Tags and Sensor Nodes, Proceedings of the second ACM conference on Wireless network security (WiSec '09) (pp. 59–68), NY, USA.

[10] Rabin, M. (1979). Digitized signatures and public key functions as intractable as factorization. Technical report, MIT, Cambridge, MA, USA.

[11] Shamir, A. (1995) Memory efficient variants of public key schemes for smart card applications. In A. D. Santis (Ed.), *Advances in Cryptology, EUROCRYPT'94,* LNCS, vol. 950, page 445–449, Springer-Verlag, Perugia, Italy.

[12] McEliece, R. (1978). A public key cryptosystem based on algebraic coding theory. *The Deep Space Network Progress Report,* (pp. 114-116), DSN PR 42–44.

[13] Niederreiter, H. (1986). Knapsack-type cryptosystems and algebraic coding theory, Problems of Control and Information Theory, 15(2), pp. 159–166.

[14] Bringer, J., Chabanne, H. and Icart, T. (2008). Cryptanalysis of EC-RAC, a RFID Identification Protocol, In M. K. Franklin, L. C. K. Hui, and D. S. Wong, (Ed.), *CANS 2008*(pp. 149–161), LNCS 5339 Springer, Hong-Kong, Chiana.

[15] Bringer, J., Chabanne, H. and Icart, T. (2009). Efficient Zero-Knowledge Identification Schemes which respect Privacy, In W. Li, W.Susilo, U. K. Tupakula, R. Safavi-Naini, and V. Varadharajan (Ed.), *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ASIACCS* (pp. 195–205), Sydney, Australia.

[16] Cayrel, P. L., Veron, P. and Alaoui, S. M. E. Y. (2011). A Zero-Knowledge Identification Scheme Based on the q-ary Syndrome Decoding Problem, In A.

Biryukov, G. Gong and D. R. Stinson (Eds.), *SAC 2010* (pp. 171–186), LNCS 6544, Ontano, Canada.

[17] Faugere, J.-C., Otmani, A., Perret, L. and Tillich, J.-P.(2010). Algebraic cryptanalysis of mcEliece variants with compact keys, In: Gilbert, H. (ed.) *EUROCRYPT 2010* (pp. 279–298), LNCS 6110, Springer, Heidelberg, France.

[18] Fiat, A. and Shamir, A. (1986). How to prove yourself: Practical solutions to identification and signature problems, In Andrew M. Odlyzko (Ed.), *Advances in Cryptology-CRYPTO'86,* (pp. 186–194), Santa Barba, California, USA.

[19] Fiat, A. and Shamir, A. (1987). Unforgeable proofs of identity, Securicom 87 (pp. 147-153). Paris, France.

[20] Feige, U., Fiat, A. and Shamir, A. (1988). Zero-knowledge proofs of identity, J. Cryptology, vol. 1(2), pp. 77–94.

[21] Gauthier Umana, V. and Leander, G. (2009). Practical key recovery attacks on two McEliece variants, *IACR ePrint Archive*, http://eprint.iacr.org/2009/509.pdf

[22] Guilion, L. C. and Quisquater, J. J. (1988). A "paradoxical" identity-based signature scheme resulting from zero knowledge, In Shafi Goldwasser, (Ed.), *Advances in Cryptology CRYPTO '88*(pp. 216–231). *8th Annual International Cryptology Conference,* Santa Barba, California, USA.

[23] Micali, S. and Shamir, A. (1988). An improvement of the Fiat-Shamir identification and signature scheme. In Shafi Goldwasser, (Ed.). *Advances in Cryptology CRYPTO '88, 8th Annual International Cryptology Conference* (pp. 244–247). Santa Barba, California, USA.

[24] Peters, C. (2009). Information-set decoding for linear codes over Fq, *ICAR Archive*: http://eprint.iacr.org/2009/589.

[25] Quisquater, J. J. and Guilion, L. (2000). The new Guilion Quisquater Scheme, *In Proceedings of the RSA 2000 conference*.

[26] Shamir, A. (1987). The search for provably secure identification schemes, Proceedings of the International Congress of Mathematicians(pp. 1488–1495), Berkeley, CA, USA.

[27] Stern, J. (1989a). A method for finding codewords of small weight. In Wolfmann, J., Cohen, G. (eds.), *Coding Theory and Applications 1988* (pp. 106–113), LNCS 388, Springer, Heidelberg, Toulon, France.

[28] Stern, J. (1989b). A method for finding codewords of small weight. In Wolfmann, J., Cohen, G. (eds.), *Coding Theory and Applications 1988* (pp. 106–113), LNCS 388, Springer, Heidelberg, Toulon, France.

[29] Stern, J.(1994). A new identification scheme based on syndrome decoding, In: Stinson, D. R. (ed.) *CRYPTO 1993* (pp. 13–21), LNCS 773, Springer, Heidelberg, Santa Barbara, California, USA.

[30] Aguilar, C., Gaborit, P. and Schrek, J. (2011). A new zero-knowledge code based identification scheme with reduced communication, *CoRR abs/1111.1644*.

[31] Chiang, J. T., Haas, J. and Hu, Y. C. (2009). Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multilateration, *Proc. Second ACM Conf. Wireless Network Security (WiSec '09)* (pp. 181–192), Zurich, Switzerland.

[32] Hancke, G. and Kuhn, M. (2005). An RFID Distance Bounding Protocol, *In Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)* (pp. 67–73), Athens.

[33] Molnar, D., Soppera, A. and Wagner, D. (2006). A scalable delegatable pseudonym protocol enabling ownership transfer of RFID tags, *In Selected Areas in Cryptography* (pp. 276–290), Kingston, ON, Canada.

[34] Saito, J., Imamoto, K. and Sakurai, K. (2005). Reassignment scheme of an RFID tags key for owner transfer, Embedded and Ubiquitous Computing (pp. 1303–1312), Nagasaki, Japan.

[35] Tippenhauer, N. and Capkun, S. (2009). Id-Based Distance Bounding and Localization, *Proc. 14th European Conf. Research in Computer Security (ESORICS '09)* (pp. 621–636), Saint-Malo, France.

[36] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M. and Ribagorda, A. (2011a). Attacking RFID Systems, In Harold F., Nozaki K., Tipton, M. (Ed.), *Information Security Management Handbook (*pp. 313–334), Auerbach Publications.

[37] Peris-Lopez, P. Orla, A., Hernandez-Castro, J. C. and Lubbe, J. C. (2011b). Flaws on RFID grouping-proofs. Guidelines for future sound protocols, *in* Journal of Network and Computer Applications, 34(3), pp. 833–845.

[38] Chandran, N., Goyal, V., Moriarty, R. and Ostrovsky, R. (2009). Position Based Cryptography, *Proc. Int'l Cryptology Conf. (CRYPTO'09)* (pp. 391–407), Santabarbara, CA, USA.

[39] Shmatikov, V. and Wang, M. H. (2007). Secure Verification of location claims with Simultaneous Distance Modification, *Proc. 12th Ann. Asian Computing Science Conf. (Asian '07)* (pp. 181–195), Doha, Qatar.

[40] Wei, Y. Yu, Z. and Guan, Y. (2013). Location verification algorithms for wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems, 24(5), pp. 938–950.

[41] Gaborit, P. and Girault, M. (2007). Lightweight code-based identification and signatures, *IEEE International Symposium on Information Theory* 2007, *ISIT 2007* (pp. 191–195), Nice.

[42] Burmester, M. and Munilla, J. (2011). Lightweight RFID Authentication with Forward and Backward Security, ACM Transactions on Information and System Security, 14 (1), pp. 11:1–11:26.

[43] Cao, T., Bertino, E. and Lei, H. (2009). Security analysis of the SASI protocol, IEEE Transactions on Dependable and Secure Computing, 6 (1), pp. 73–77.

[44] Sun, H.-M., Ting, W. C., and Wang, K. H. (2011). On the security of Chien's ultralightweight RFID authentication protocol, IEEE Transaction on Dependable and Secure Computing, 8 (2), pp. 315–317.

[45] Juels A. (2005). RFID security and privacy: A research survey, IEEE Journal on Selected Areas in Communication, 24 (2), pp. 381–394.

[46] Koh, R., Schuster, E. and Chackrabarti, I. (2003). A. Bellman, Securing the pharmaceutical supply chain, White Paper, Auto-ID Labs, Massachusetts Institute of Technology.

[47] Takaragi, K. Usami, M., Imura, R., Itsuki, R. and Satoh, T. (2001). An ultra small individual recognition security chip, IEEE Micro, 21(6), pp. 43–49.

[48] Lehtonem, M., Staake, T., Michahelles, F. and Fleisch, E. (2007). From Identification to Authentication-A Review of RFID Product Authentication Techniues, *Networked RFID Systems and Lightweight Cryptography,* P. H. Cole, D. C. Ranasinghe (Ed.), pp. 169–187.

[49] Yu, S., Ren, K. and Lou, W. (2007) A Privacy-preserving Lightweight

Authentication Protocol for Low-Cost RFID Tags. *Military Communication Conference, MILCOM 2007* (pp. 1–7), Orlando, FL, USA.

[50] Burmester, M., Le, T. V. and Medeiros, B. D. (2009). Universally Composable RFID Identification and Authentication Protocols, *ACM Transaction on Information and Systems Security*, 2(4), pp. 21:1–21:33.

[51] Mitra, M. (2008). Privacy for RFID systems to prevent tracking and cloning, International Journal of Computer Science and Network Security, 8(1), pp. 1–5.

[52] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., Li, T. and Lubbe, J. C. A. van Der, (2010). Weaknesses in Two Recent Lightweight RFID Authentication Protocols, Information Security and Cryptology (pp. 383–392), Beijing, China.

[53] Tian, Y., Chen G. and Li, J. (May 2012). A New Ultralightweight RFID Authentication Protocol with Permutation, IEEE Communications Letters, 16(5), pp. 702–705.

[54] Haber, S. and Stornetta, W.(1991). How to time-stamp a digital document, Journal of Cryptology, 3(2), pp. 99–111.

[55] Deursen TV and Radomirovie S. (2010). EC-RAC: Enriching a Capacious RFID Attack Collection, RFIDSec 2010 (pp. 75–90), Istanbul, Turkey.

[56] Fan, J., Hermans, J. and Vercauteren, F. (2010). On the claimed privacy of EC-RAC III, RFIDSec 2010 (pp. 66–74), Istanbul, Turkey.

[57] Chien, H. Y. and Liu, S. B. (2009). Tree-Based RFID Yoking Proof, *International conference on Networks Security,* Wireless Communications and Trusted Computing (NSWCTC'09), pp. 550–553.

[58] Due, D. N. and Kim, K. (2009). Grouping-proof protocol for rfid tags: Security definition and scalable construction, *Cryptology ePrint Archive*, Report 2009/609, http://eprint.iacr.org/

[59] Burmester, M., de Medeiros, B. and Motta, R. (2008). Provably Secure Grouping Proofs for RFID Tags, Proceedings of the 8th Smart Card Research and Advanced Applications-CARDIS 2008(pp. 176–190), Springer, Royal Holloway University of London, UK.

[60] Cheng, Z. Y., Liu, Y., Chang, C. C. and Chang, S.C. (2013). Authenticated RFID security mechanism based on chaotic maps, Security and Communication Networks, 6(2), pp. 247–256.

[61] Akgun, M. and Caglayan, M. U. (2013). Weaknesses in a Recently Proposed RFID Authentication Protocol, *IACR Cryptology ePrint Archive:* https://eprint.iacr.org/2013/855.

[62] Biasi, F. P., Barreto, S. L. M. B., Misoczki, R. and Ruggiero, W. V. (2012). Scaling efficient code-based cryptosystems for embedded platforms, *CoRR, abs/1212.4317*

[63] Mujahid, U., Najam-ul-islam, M., Ahmed, J. and Mujahid, Us. (2013). Cryptanalysis of ultralightweight RFID authentication protocol, *Cryptology ePrint Archive,* Report 2013/385.

[64] Pearson, J. (2005). Securing the pharmaceutical supply chain with RFID and public key infrastructure (PKI) technologies, Texas instruments White Paper, Available from: http://www.ti.com/rfid/docs/docntr.shtml

[65] Nochta, Z., Staake, T. and Fleisch, E. (2006). Product Specific Security Features Based on RFID Technology, International Symposium on Applications and the Internet

Workshops (SAINTW'06), 2006 (pp. 72-75).Phoenix, AZ.

[66] Qingling, C., Yiju, Z. And Yonghua, W. (2008). A minimalist mutual authentication protocol for RFID system and BAN logic analysis. *CCCM 2008* (pp. 449–453), Guangzhou.

[67] Liu, Y., Qin, X., Wang, C. and Li, B. (2013). A Lightweight RFID Authentication Protocol based on Elliptic Curve Cryptography, Journal of Computers, 8(11), pp. 2880–2887.

[68] Cho, J.-S., Yeo, S.-S, Hwang, S., Rhee, S.-Y. And Kim, S. K. (2008). Enhanced yoking proof protocols for RFID tags and tag groups. *International Conference on Advanced Information Networking and Applications- Workshop-AINAW 2008* (pp. 1591–1596), IEEE Computer Society, Okinawa, Japan, pp. 1591–1596.

[69] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M. and Ribagords, A. (2007). Solving the Simultaneous Scanning Problem Anonymously: Clumping Proofs for RFID Tags, In IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing-SecPerU 2007(pp. 55–60), IEEE, IEEE Computer Society Press, Istanbul, Turkey.

[70] Piramuthu, S. (2006). On Existence Proofs for Multiple RFID Tags, *IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing –SecPerU 2006,* IEEE, IEEE Computer Society Press, Lyon, France.

[71] Juels, A. (2004). Yoking-Proofs for RFID Tags, In: Sandhu, R., Thomas, R. (Eds.), *International Workshop on Pervasive Computing and Communication Security- PerSec 2004* (pp. 138–143), IEEE, IEEE Computer Society, Orlando, Florida, USA.

[72] Juels, A. (2006). RFID Security and Privacy: A Research Survey, IEEE Journals on Selected Area in Communications, 24(2), pp. 381–394.

[73] Lin, E.-C., Lai, Y.-C., Tygar, J. D., Yang, C.-K. and Chiang, C.-L. (2007). Coexistence proof using chain of timestamps for multiple RFID tags, In: Chang, K. C.-C., Wang, W., Chen, L., Ellis, C. A., Hsu, C.-H., Tsoi, A. C., Wang, H. (Eds.), *International Workshop on DataBase Management and Application over Networks – DBMAN 2007* (pp. 634–643), LNCS 4537, Springer-Verlag, Huang Shan, China.

[74] Saito, J. and Sakurai, K. (2005). Grouping Proof for RFID Tags, *International Conference on Advanced Information Networking and Applications-AINA*, (pp. 621–624), Taiwan.

[75] Bagheri, N. And Safkhani, M. (2013). Secret Disclosure attack on Kazahaya, a Yoking-Proof For Low-Cost RFID Tags, *IACR Cryptology ePrint Archive 2013*: 453. https://eprint.iacr.org/2013/453.pdf

[76] Hung-Yu Chein and Chen-Wei Huang. (2007). A lightweight RFID protocol using substring, In Embedded and Ubiquitous Computing (EUC 2007) (pp. 422–431), Taipei, Taiwan.

[77] Ahmadian, Z., Salmasizadeh, M. and Reza Aref, M. (2013). Desynchronization Attack on RAPP Ultralightweight Authhentication Protocol, Information Processing Letters, 113(7), pp. 206–209.