Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 14 (2019) pp. 001-010
© MIR Labs, www.mirlabs.net/jias/index.html

Comparative Analysis of Multi-round Cryptographic Primitives based Lightweight Authentication Protocols for RFID-Sensor Integrated MANETs

Adarsh Kumar[1], Saurabh Jain[2] and Alok Aggarwal[3]

[1,2,3] School of Computer Science, Department of Systemics, University of Petroleum and Energy Studies
Bidholi Campus, Dehradun, India
[1]adarsh.kumar@ddn.upes.ac.in, [2]saurabh.jain@ddn.upes.ac.in, [3]alok.aggarwal@ddn.upes.ac.in

Abstract: **Authentication is among the initial process of reliable network construction and formulization. This process is necessary for all types of networks including re-sourceful and resource constrained devices. Various authentication protocols are available for resourceful devices but resource constrained devices demands high security authentication protocols with least computational and communicational costs. Among cryptography protocols based protocols, elliptic curve cryptography (ECC) based authentication protocols ensures high security as compared to other protocols. In this work, ECC based authentication protocols are identified and their performance is analyzed with variable number of nodes in the network. This study analysis the feasibility of ECC based authentication protocols for re-source-constrained devices. In simulation, 8 ECC based authentication protocols are analyzed for networks with different sizes (50 to 1000 nodes). In results, a minimum of 4.3% (50 nodes network) and maximum of 12.9% (for 1000 nodes network) improvement is observed for protocol 5 as compared to other protocols.**

Keywords: RFID system, Reader, Tag, Authentication protocols, Simulation, QoS.

I. Introduction

The term, Internet of things, refers to uniquely addressable objects and their inter-connection in an Internet like structure. These uniquely addressable objects may transmit real time sensor data about the physical state of the object, other useful properties of these objects. Objects can be pacemakers, motor vehicles, smart bill boards, wirelessly connected pill shaped cameras in digestive tracks, refrigerators, televisions, air-conditioners or even humans and cattle etc. which can be equipped with various kind of sensors which helps in getting useful information about these objects. Major features of an IoT are automatic identification, sensing, self configuration, intelligent decision making, adhoc networking etc. In an IoT network for peer-to-peer communication and functionality, each device being connected requires its own IP address. A 32-bit address has been used in the originally developed internet protocol IPv4 with which a maximum of 4.3 billion devices can be connected. However in case of IoT total number of devices connected to each other has already crossed the world's population of seven plus billion about one decade back. Hence IPv4 is nowhere feasible for IoT. IPv6 protocol has 128-bit address and hence has an address space of 2^{128} which is likely to solve the unique addressability issue of IoT phenomena.

Scalability, distributed processing and security continues to be among the most challenging issues of IoT. Since large number of connected devices are generating data in an automated way and it will largely dwarf the information which individuals can enter manually. Amount of data an individual can enter into the system when a huge number of devices are connected in an IoT, is limited by time and physical limits of an individual and is unlikely to change very much over time. On the other hand, amount of effectively collected data from embedded sensor devices is steadily increasing due to recent advancements in hardware technology. Further, huge data generated by social media like facebook, whatsapp etc. is adding further to this scalability issue of IoT and has been the greatest driving force for big data analytics.

Apart from scalability issue, data security is another major challenging issue of IoT. Objects can be tracked and when associated with individuals can lead to privacy and security problems. Objects are uniquely addressed and identified in IoT, RFID being a preferred choice for this. Environmental information is sensed by these objects which is communicated to other connected objects through Internet. RFID techniology allows a sensor to read a unique product identification code associated with a tag from a distance without line-of-sight. The unique code is transmitted to one or more sensors or readers which, in turn, transmit the reading to one or more sensors. Later the collected data is aggregated at the server. RFID tags are powered by sensor readers and hence do not require the battery power for their operation. Due to which distance between RFID tags and readers can not be very long for effective reading. A wide variety of objects is used in IoT like sensors, RFID tags, short range wireless connectivity, mobile devices, backend storage etc. These are classified into two broad categories; resourceful & resource constraint devices. Resourceful devices have sufficient computational, storage capabilities while resource constraint devices lack in hardware and software resources. RFID technology has various limitations from the data centric perspective like limited sensing capabilities especially when passive tags are used, very short range of tags from 5-20 meters, noisy/incomplete/redundant data collection etc. Further, from the privacy perspective, if tags are associated with individuals then this technology may give a considerable privacy challenge since covert readers can be used to track the location of individuals. RFID systems have become a very common tool in inventory control, supply chain management, industrial manufacturing process and even in cattle herding for automatic object identification. RFID systems have taken a clear-cut lead and almost fully replaced by earlier optical barcodes which were designed in early seventies and found since than on many products. Recent advancements in silicon manufacturing has given a boost to RFID systems by offering very low cost RFID devices and consequently helped RFID technology as an economical replacement for optical barcodes.

Tags are small memory devices with limited storage capacity which stores identification types and other specifications of objects. Data size is very limited upto 2-3 KB only. Analog signal of sensor devices is converted to digital form and read by readers. Readers may use infrastructure or infrastructure-less networks for processing and storing the read information in a backend system. Tags are of various types; passive, active or a combination of both. Active tags have their own battery and transmitting source and are comparatively costlier to passive tags which do not have own battery source. Passive tags get the power to operate or transmit from the destination through electromagnetic waves. Active tags have a longer transmitting range compared to passive tags and are preferred to identify objects over long distances such as in healthcare applications, animal tracking, object locating in logistics market or in traffic congestion management. For short range application, passive tags are preferred due to their low cost. Semi-passive tags have their own battery source but consumes destination energy for communication from electromagnetic waves. Readers read the information of tags for object identification and record management and sends this read information to backend systems for further process. Wireless sensor devices are integrated with RFID devices for increasing the availability of the data range. Both RFID devices and sensor networks are pervasive environments and integration of these two gives a reliable energy efficiency, sustainable and cost effective solutions to many applications.

Authentication is one of the major security aspect for all systems including RFID-sensor integrated MANET. Authentication protocols allow only valid users as a part of the system and unauthorized users are discarded. Standard cryptographic algorithms, be it symmetric or asymmetric, can support authentication protocols. Both, standard symmetric encryption algorithms like DES, AES etc. or standard asymmetric encryption algorithms like RSA are not feasible from authentication perspective for an RFID-sensor integrated MANET. Tens of thousands of gate equivalents (GEs) are needed for implementing RSA, DSA or AES algorithms while RFID-sensor integrated MANET could hardly afford 2K to 3K GEs for security perspective due to its low cost. Further, these asymmetric or symmetric standard cryptographic algorithms also requires ample storage space for keys, making these algorithms not feasible for a RFID-sensor integrated MANET. Recently, however, a lightweight AES required only approximately 4K GEs but still not feasible for RFID devices. About one-third of total GEs are available for lightweight cryptographic primitives and protocols in a resource constraint device [1]-[2]. Resources available in a low cost RFID devices are quite less what is necessarily required for standard public key cryptography even for a resource-efficient scheme like NTRU [3]-[4] or SHA-1 [5]. Even Tiny Encryption Algorithm [6]-[7] is also not feasible for these resource constraint RFID devices. All these factors forces for a lightweight or ultra-lightweight cryptography.

Lightweight cryptography is classified as pre-quantum cryptography, post quantum cryptography and lightweight protocols. Pre-quantum cryptography is further classified as symmetric and asymmetric cryptography. Symmetric pre-quantum lightweight cryptography consists of stream ciphers, block ciphers, hash functions and random number generators while asymmetric pre-quantum lightweight cryptography consists of BlueJay, elliptic curve cryptography (ECC), hyper elliptic curve cryptography (HECC), and NTRU. Post-quantum lightweight cryptography could be lattice, hash, code or multi-variate based. Lightweight protocols are classified as identification, authentication, distance bounding, grouping proof and tag ownership. ECC was proposed in 1985 by Victor Miller et al. [60] and has various strengths like it requires smaller key sizes and greater flexibility, provides high speed and requires less storage space for its operation making it feasible for resource constraint devices and it is mainly used in key exchange, digital signature authentication etc. ECC requires about 8K GEs with area 0.18 µm technology. HECC was proposed in 1989 by Koblitz and has various strengths like faster key generation, reduced cost as disposable keys are reused, less memory usage making it feasible for resource constraint devices and a lattice based cryptosystem. HECC requires about 14.5K GEs with 0.13 µm technology.

As shown in fig. 1 to fig. 3, lightweight authentication protocols in RFID systems can use anyone of the self-explained basic strategies with different mathematical computations at reader, tag or data centre side.

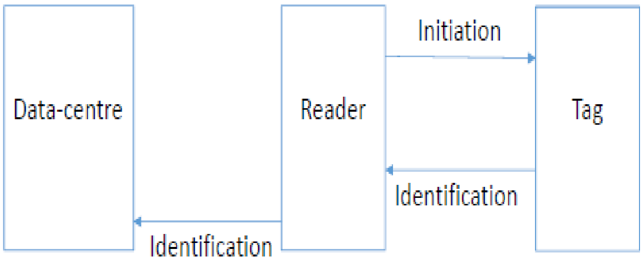

Figure 1: Process 1 of authentication in RFID system

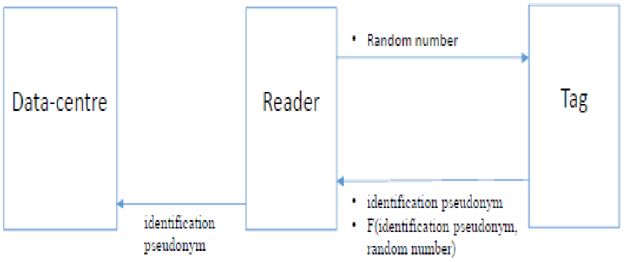

Figure 2: Process 2 of authentication in RFID system

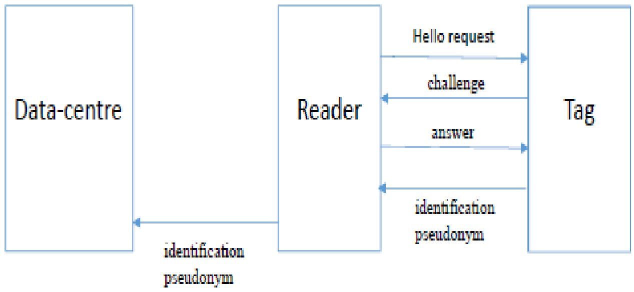

Figure 3: Process3 of authentication in RFID system

In this work, lightweight authentication protocols are evaluated for resource-constrained devices. These authentication protocols are elliptic curve cryptography based multi-round protocols with quadratic equations. This work is an extension to the work presented by Kumar *et al.* [82] for RFID system having reader and tag for identification and interrogation with different network sizes. Hierarchical network construction is a process involving a group of nodes in close vicinity to interconnect among themselves using authentication protocols. Each group has a leader to execute this process. Further, a comparative analysis of elliptic curve cryptosystem based authentication protocols is performed to identify best protocol having higher QoS. In simulation, a network of 50 to 1000 nodes is consider for performance analysis.

Rest of the paper is organized as follows. Section 2 gives in brief a summary of the works done by earlier researchers for authentication protocols based on elliptic curve cryptosystem for RFID-sensor integrated MANET. Section 3 discusses various ECC based authentication protocols in details. Discussions in this section consider resource constrained environment for RFID system. In section 4, simulation is performed for authentication protocols with 50 to 1000 nodes networks. This section shows a comparative analysis of protocols taken into consideration. Finally, section 5 concludes the work.

II. Literature Survey

Security of RFID tags remains a challenging issue due to their resource constraint nature and also of physical form. Many technical features of RFID tags like gate count upto 10K, security gate count upto one-third of total gate count, operating frequency in UHF range, clock cycles per read upto 10K, usually passively powered tags, power consumption of 10 µwatts, upto 512 bits of ROM storage and upto 128-bits RW memory makes them highly resource constraint. Privacy or authentication in RFID systems have been proposed initially without any standard cryptographic primitives of tags by many researchers, e.g., [8]-[13]. Symmetric key primitives have been proposed by researchers for authentication purpose in RFID, e.g., [13]-[18]. A low cost AES implementation have been proposed in [19] by Dominiku et al. Many researchers have proposed a human authentication protocols for RFID devices [20]-[26]. Matsumoto et al. [22]-[23] have proposed a human authentication protocol for RFID devices which is good enough for small number of authentication [25]. Naor et al. [24] have proposed a human authentication protocol based on virtual reality which provides security against passive eavesdropping however failed to provide security against active attackers. Hopper at el. [20]-[21] also proposed similar authentication protocol by covering limitation of security against active attackers. Ari Juels et al. [26] have extended the work proposed in [20]-[21] for human authentication protocol and proposed an augmented version of the Hopper & Blum (HB) protocol, named as HB$^+$ which is secure against active adversaries. Proposed protocol is a symmetric lightweight authentication protocol with simple and low cost implementations. It is claimed that the proposed HB$^+$ protocol is secure against passive eavesdropping and adversaries. Authors in [27] have discussed cautionary information while implementing AES for authentication in smart cards. Authors in [28]-[31] have pointed out that RFID devices are highly susceptible to various attacks like timing attack, power analysis attacks and to fault induction too especially when passive RFID tags are used. Authors in [4] have addressed the location privacy risks in Bluetooth technology which is equally relevant to RFID systems. Authors in [32] have given an analysis of smart card operation in hostile environments.

Privacy issue in RFID device has been addressed by many earlier works [33]-[50] in case when RFID tags are associated with individuals. For RFID devices most of the work in data-centric pipeline has three primary visions; things-oriented vision [51]-[54], Internet-oriented vision [55]-[58] and semantic-oriented vision. The most dominant vision today is things-oriented vision which supports electronic product code in conjunction with RFID technology to collect and track sensor data. The internet-oriented vision addresses to the construction of the IP protocols for enabling smart connected objects while semantic-oriented vision addresses the issues of data management.

Various asymmetric lightweight protocols have been developed which are reasonably suitable for RFID devices like NTRU by Jeffrey Hoffstein et al. [3], BlueJay by Markku-Juhani O. Saarinen [59], ECC by Victor Miller et al. [60] and HECC by Koblitz. Authentication is a mechanism used for validity of message between RFID tags and readers. Lightweight authentication protocols for RFID devices are broadly divided into four major categories: : (a) protocols based on cryptographic primitives, (b) protocols based on ultra lightweight operations, (c) protocols based on the capabilities of EPCglobal Class1 Generation2 and (d) protocols based on the notion of physical primitives [61]. Protocols based on ultra-lightweight operations authenticate product with tag or without tag. Authenticating product without tag could be done in two ways; by unique serial number [62]-[65] or track with trace based plausibility check [65]-[66]. Physical property based authentication approach has been presented in [67]. Protocols based on the notion of capabilities of EPC global class1 Generation2 are based on hashing, pseudo random number generation and specific security model based requirements [68]. Many of these protocols are susceptible to man-in-middle, de-synchronization, traceability, cracking codes using binary operation [69]-[76]. Various hash based protocols like RIP, ROP, O-RAP etc. have been developed to cover traceability [77]-[81].

III. ECC BASED AUTHENTICATION PROTOCOLS

In this section, mathematics of ECC based authentication protocols are explored for resource-constrained devices in IoTs. Detailed working of RFID reader and tag integrated authentication protocols are discussed as follows:

Protocol 1: User authentication using ECC Encryption/Decryption Cryptography Primitive.

Step 1:- In first step, reader 'R' selects a random number 'r_1' and generates its message digest 'H' using some hashing algorithm. It also encrypts identification of tag ID_T with the help of 'r_1' and generates cipherext 'C_R'. Reader sends ciphertext, identification of tag and message digest to tag.

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:- Tag 'T' decrypts the ciphertext received and obtains message digest and identification. It compares the received identification with its own identification. If it matches then re-generates the message digest and compare with received digest. After comparison, tag resends 'y' to reader.

T : $(y,ID_T)=D(C_R)$
: Verify [h(y)==H] and [decrypted ID_T is same as of its own ID], if verified then
T→R : y

Step 3:- Reader compares the received message with generated random number. If both matches then reader is ensured that tag is authentic.

R : if $y==r_1$ then user with tag 'T' is considered to be authentic else unauthentic.

Protocol 2: User authentication using ECC based signature generation and verification.

Step 1:- In first step of this protocol, Reader 'R' sends a random number 'r_1' to tag 'T'.

R→T : r_1

Step 2:- Tag digitally signs the received random number, a newly generated random number 'e_1' and identification of reader. Tag sends new random number, identification of reader, digitally signed message and certificate of tag to reader.

T : $y = SIGN(r_1, e_1, ID_r)$
T→R : e_1, ID_r, y, $CERT_{TAG}$

Step 3:- Finally, reader matches both the certificate and digitally signed message. If both matches then tag is considered to authentic else un-authentic.

R : VERIFY $CERT_{TAG}$ and VERIFY y
: if both are verified then tag is authentic else unauthentic

Protocol 3: Authentication Protocol using ECC and Schnorr Identification scheme.

Step 1:- Tag 'T' computes a challenge 'X' and sends it to reader 'R'.

T : Computer $X=r_1P$
T→R : X

Step 2:- Reader responses with a random number.

R→T : e_1

Step 3:- Now**,** reader generates a new challenge to reader with the help of constant 'a', reader random number 'e_1' and tag random number 'r_1'.

T : Compute $y=ae_1+ r_1$
T→R : y

Step 4:- Reader verifies the challenge with received response 'y', base point 'P' of elliptic curve 'E', random number 'e_1 and tag's public key 'Z'. If the result matches with the initial response then tag is considered to authentic else unauthentic.

R : if $yP+ e_1Z==X$ then authentic else unauthentic

Protocol 4: Authentication Protocol using ECC and Okamoto's Identification scheme.

Step 1:- Tag 'T' generates a challenge using random numbers 'e_1' and 'e_2', and points on elliptic curve P_1 and P_2. Tag sends this challenge 'X' to reader 'R'.

T : Computes $X=e_1P_1 + e_2P_2$
T→R : X

Step 2:- Reader 'r' sends a random number 'r_1' response to tag.

R→T : r_1

Step 3:- Now, tag generates two new challenge 'y_1' and 'y_2'. New challenges are generated with the help of random number selected by tag i.e. 'e_1' and 'e_2', random number selected by reader i.e. 'r_1' and 'r_2', and points on curve 's_1' and 's_2'. Tag sends these challenges to reader.

T : Computes $y_1= e_1+r_1s_1$ and $y_2= e_2+r_1s_2$
T→R : y_1, y_2

Step 4:- Reader verifies the response with tag's public key 'Z'. If it matches with initial challenge (step 1) then tag is considered to be authentic else un-authentic.

R : Computes $y_1P_1 + y_2P_2+ r_1Z$
: if $y_1P_1 + y_2P_2+ r_1Z$ equals to X then authentic else unauthentic.

Protocol 5: EC-RAC 1

Step 1:- Tag generates a challenge for reader with the help of random number e_1 and base point selected on elliptic curve 'P'. This challenge is send to reader.

T→R : e_1P

Step 2:- Reader sends a new random number response to tag i.e. r_1.

R→T : r_1

Step 3:- Tag reconsider a new challenge with the help of random numbers 'e_1' (from tag) and 'r_1' (from reader), identification of tag, and public key of reader. Tag sends this new challenge to reader.

T : $Temp = (e_1+r_1ID^T) PU^R$
T→R : Temp

Step 4:- Reader verifies the new received challenge with private key ‘PR^{R}’ of its own. If challenge is verified then tag is considered to authentic else un-authentic.

R : $((PR^{R})^{-1}Temp - e_1P)r_1^{-1} = ID^{T}P$

Protocol 6: EC-RAC 2

Step 1:- Tag ‘T’ generates a challenge with the help of random number ‘e_1’ and base point on elliptic curve ‘E’. Tag sends this challenge to reader ‘R’.

T→R : e_1P

Step 2:- Reader generates a random number ‘r_1’ and sends it to tag.

R→T : r_1

Step 3:- Tag computes two challenges ‘$Temp_1$’ and ‘$Temp_2$’ with the help of random numbers (e_1 and r_1), password of tag stored at data centre ($PASSWD^{T}$), identification of tag (ID^{T}) and public key of reader (PU^{R}). Tag sends these challenges to reader.

T : $Temp_1 = (e_1+r_1ID^{T})PU^{R}$, $Temp_2 = (e_1ID^{T} + r_1PASSWD^{T}).\ PU^{R}$

T→R : $Temp_1$, $Temp_2$

Step 4:- Reader verifies received challenges with the help of password verifier (**(**$PASSWD\text{-}VERIF^{T}$), private key of reader (PR^{R}) and inverse operations. If challenge is verifies then tag is considered to authentic else un-authentic.

R : $((PR^{R})^{-1}Temp_1 - e_1P)r_1^{-1} = ID^{T}P$, Now find ID^{T} entry and extract $PASSWD\text{-}VERIF^{T}$.

: if $((PR^{R})^{-1}Temp_2 - ID^{T}.e_1.P)\ r_1^{-1}$ equals to $PASSWD\text{-}VERIF^{T}$ then accept else reject.

Protocol 7: EC-RAC 3

Step 1:- In first step, tag ‘T’ computes two challenges for reader with random numbers e_1 and e_2, and base point on elliptic curve ‘P’. Tag sends these challenges to reader.

T→R : e_1P, e_2P

Step 2:- Reader ‘R’ reply back with a random number to tag.

R→T : r_1

Step 3:- Tag generates two challenges with the help of tag selected random numbers (e_1 and e_2), reader selected random number (r_1), tag password stored in data centre ($PASSWD^{T}$), identification of tag (ID^{T}) and public key of reader (PU^{R}). Tag sends these challenges to reader.

T : $Temp_1 = (e_1+r_1ID^{T})PU^{R}$, $Temp_2 = (e_2ID^{T} + r_1PASSWD^{T}).\ PU^{R}$

T→R : $Temp_1$, $Temp_2$

Step 4:- Reader verifies the received challenges with the help of its own private key (PR^{R}), random number (e_1 and r_1), password verifier ($PASSWD\text{-}VERIF^{T}$) and inverse operations. If challenges are verified then tag is considered to authentic else un-authentic.

R : $((PR^{R})^{-1}Temp_1 - e_1P)r_1^{-1} = ID^{T}P$, Now find ID^{T} entry and extract $PASSWD\text{-}VERIF^{T}$.

: if $((PR^{R})^{-1}Temp_2 - ID^{T}.e_2.P)\ r_1^{-1}$ equals to $PASSWD\text{-}VERIF^{T}$ then accept else reject.

Protocol 8: ERAP (ECC based RFID Authentication Protocol).

Step 1:- Reader generates a random number challenge ‘r_1’ and sends it to tag ‘T’.

R→T : r_1

Step 2:- First, Tag computes a point ‘P’ using a new random number ‘e_1’ and generator on elliptic curve ‘G’. Another coordinate (x_T, y_T) is calculated from (x_p, y_p) using ‘e_1’, ‘r_1’, private key of tag i.e. PR_T ($=e_3$) and inverse operations. Tag reply back with new coordinates (x_T, y_T) and new random number ‘e_2’.

T : Compute $P=e_1G= (x_p, y_p)$

: if $x_p \in F_n$ then $x_P^I \in [1,n-1]$ else if $x_P^I \in F_{2^n}$ then $x_P^I = \sum_{i=0}^{n-1} 2^i x_P$

: Compute $x_T = x_P^I$ mod n and $y_T = e_1^{-1}(r_1+PR_T.\ x_T)$

: if x_T or y_T is zero then recalculate step 2.

T→R : (x_T, y_T) and e_2

Step 3:- Initially, received coordinates are verified i.e. whether x_T and $y_T \in [1,n-1]$. If any of these coordinates is not verified then tag is considered to un-authentic else authentic and continues. Reader uses $PU_T(=e_3G)$ i.e. the public key of tag to generate a new challenge for tag (x_R, y_R). Reader sends this challenge to tag.

R : Compute $w= (y_T)^{-1}$mod n, $u_1=r_1w$ mod n, $u_2= x_Tw$ mod n and $P' = u_1G+ u_2 .PU_T$. if $P'=\infty$ then tag is considered to be unauthentic else continue.

: if $x_{P'} \in F_n$ then $x_{P'}^I \in [1,n-1]$ else if $x_{P'}^I \in F_{2^n}$ then $x_{P'}^I = \sum_{i=0}^{n-1} 2^i x_{P'}$

: Now, if $x_T = x_{P'}^I$mod n then tag is authentic else unauthentic.

: Authentic tag will compute $P'' = r_2PU_T$ and if $x_{P''} \in F_n$ then $x_{P''}^I \in [1,n-1]$ else if $x_{P''}^I \in F_{2^n}$ then $x_{P''}^I = \sum_{i=0}^{n-1} 2^i x_{P''}$, $x_R = x_{P''}^I$ mod n, $y_R = r_2^{-1}(e_2+PR_Rx_R)$ mod n, if x_R or y_R is zero then recomputed these variables by selecting another value of r_2 and computing P''.

R→ T : (x_R, y_R)

Step 4:- Here, tag also verifies that whether x_R and $y_R \in [1,n-1]$, if anyone is not verified then tag is considered to unauthentic else authentic and continues. Tag computes a point P' using the seed used to randomly generate the elliptic curve i.e. ‘S’. It checks the range of P'. If P' lies within acceptable range then tag is considered to be authentic else un-authentic.

T : Compute $w= (y_R)^{-1}$mod n, $u_1=e_1w$ mod n, $u_2= x_Rw$ mod n and $P' = (u_1+ u_2S)\ PR_T\ G$. if $P'=\infty$ then tag is considered to be unauthentic else continue.

: if $x_{P'} \in F_n$ then $x_{P'}^I \in [1,n-1]$ else if $x_{P'}^I \in F_{2^n}$ then $x_{P'}^I = \sum_{i=0}^{n-1} 2^i x_{P'}$

: Now, if $x_R = x_{P'}^I$mod n then tag is authentic else unauthentic.

IV. Results and Analysis

A detailed simulation analysis of small scale (50 nodes) to large scale network (1000 nodes) is performed in this section. An open-source and discrete-events simulator is used for analyzing the network performance. Details of simulation, execution, results interpretations and their analysis is presented as follows:

***Simulation Parameters*:** In simulation, various parameters are selected that supports hierarchical network structure formation. These parameters are shown in table 1. A set of nodes is divided into groups and groups are interconnected through cluster head. Group head is programmed to have reader capacity with nodes scanned through tags. These tags stores unique identities with independent scanning.

Table 1: Simulation Parameters

Parameter	**Value**
Type of Channel used	WirelessChannel
Radio Propagation Model	TwoRayGround
Network Interface	WirelessPhy
MAC Type	802.11
Type of Queue used for packet storage	Priority Queue
Antenna	OmniAntenna
Max Number of Packets that can be stored in a Queue	50
Routing Protocol	ZRP
X dimension of the topogra-phy	1000 meters
Y dimension of the topogra-phy	1000 meters
Mobility Model	Random WayPoint Mobili-ty
Data Rates	5 packets/second
Packet Size	512 bits
Simulator	ns-3
Simulation Time	1000sec

Jitter: It is measured as the deviation in delay while transmitting packets. Increase in delay is not heathy for efficient network performance. Fig. 4 to fig. 7 shows the jitter value analysis for 50 to 200 nodes network. For 50 nodes network, protocol 2 to protocol 6 are better than protocol 1, protocol 7 and protocol 8 for all data rates. Protocol 1 is giving overall best performance because of least computational efforts is required for complete authentication process. For 75 nodes network, protocol 1 to protocol 6 are better than protocol 7 and protocol 8. Out of protocol 1 to protocol 6, protocol 5 is giving better performance but this performance is comparable with protocol 1, protocol 3 and protocol 4. For protocol 1 to protocol 6, jitter is minimum with packet rate of 5 pkt/sec. However, jitter is minimum for protocol 7 and protocol 8 with packet rate of 0.1 pkt/sec., and maximum with packet rate of 5 pkt/sec. For 150 nodes network, trends are same as of a network consisting of 75 nodes. Protocol 1 to protocol 5 are performing better as compared to protocol 6 to protocol 8. In this scenario, protocol 5 is evaluated to be the best protocol as compared to all other protocols. Among protocol 1 to protocol 5, higher packet rate (5 pkt/sec) is reliable and give least jitter value. Similarly, protocol 7 and protocol 8 are observed to be the best with packet rate of 5 pkt/sec. Protocol 6 performed better with lower packet rate (0.1 pkt/sec.) because of internal manipulations with packets while processing. Overall, higher packet rate is preferred for 150 nodes network. For 200 nodes network, all protocols except protocol 3 and protocol 6 perform better with packet rate of 1 pkt/sec. Protocol 3 and protocol 6 is good with 0.1 pkt/sec. With increase in number of nodes, neither lower nor higher packet rate is preferred because of increases in number of packets over the network. Thus, a medium rate provides efficient performance. In another observation, it is found that protocol 1, protocol 2, protocol 4 and protocol 8 increases performance with increase in data rate and number of nodes present in the network.

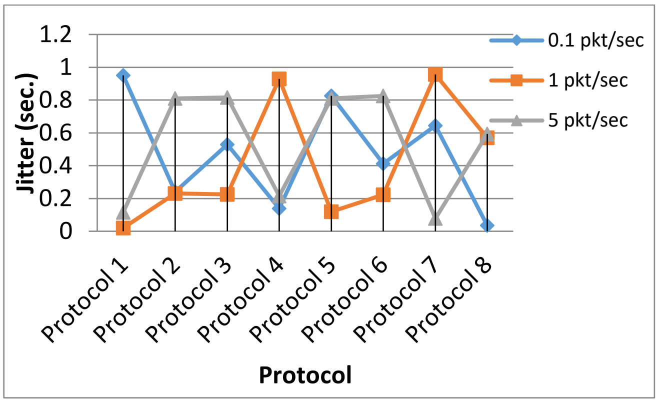

Figure 4: Comparative jitter analysis of ECC based authentication protocols for 50 nodes.

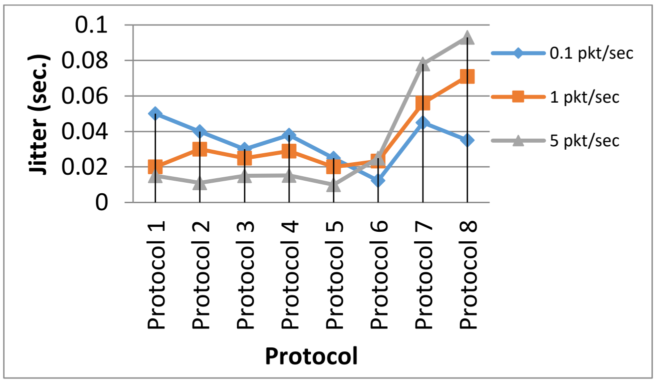

Figure 5: Comparative jitter analysis of ECC based authentication protocols for 75 nodes.

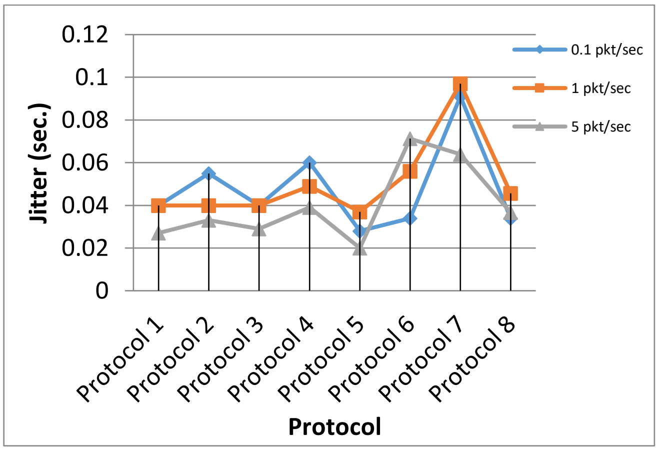

Figure 6: Comparative jitter analysis of ECC based authentication protocols for 150 nodes.

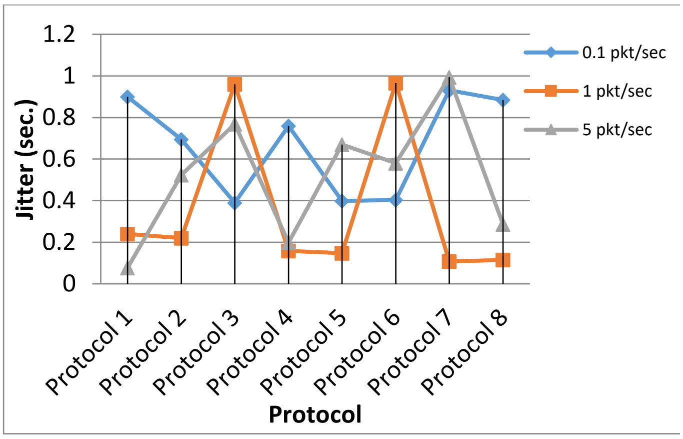

Figure 7: Comparative jitter analysis of ECC based authentication protocols for 200 nodes.

Goodput: In goodput computation, data is separated from packet header in computing the number of unit transmitted successfully to its destination per unit time. Fig. 8 to fig. 11 shows the comparative analysis of goodput computation for ECC based authentication protocol for 50 to 200 nodes networks. Overall, it is observed that goodput increases with increase in number of nodes and transmissions over the network. Protocol 5 shows maximum of 12.9% improvement for 75 nodes and minimum of 4.3% for 150 nodes as compared to other protocols. In goodput analysis, it is observed that performance is increasing with increase in number of nodes and use of protocol 5 because more routes are available with least computational overhead for packet delivery.

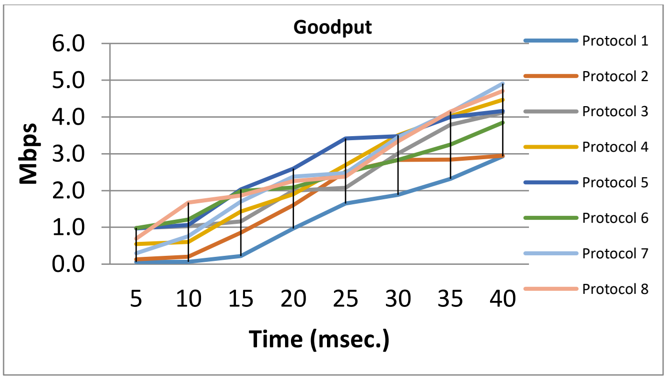

Figure 8: Comparative good analysis of ECC based authentication protocols for 50 nodes.

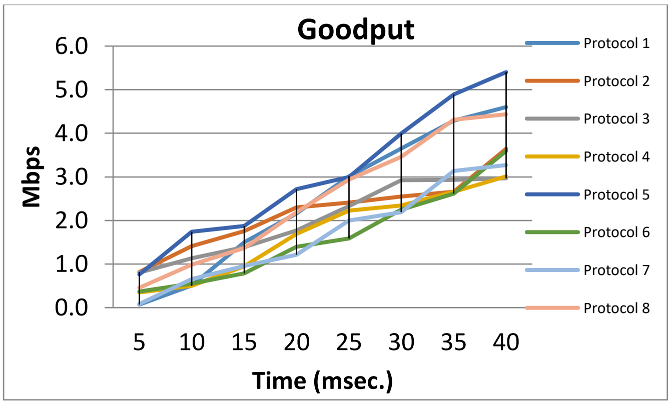

Figure 9: Comparative good analysis of ECC based authentication protocols for 75 nodes.

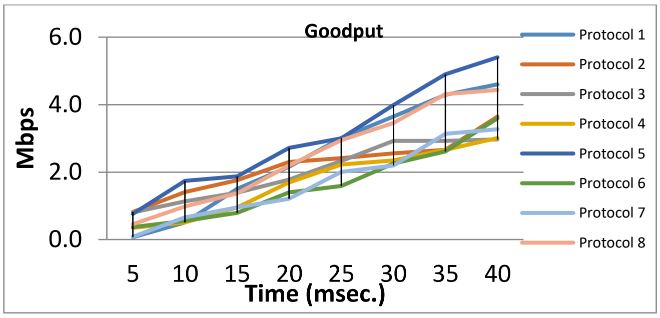

Figure 10: Comparative good analysis of ECC based authentication protocols for 150 nodes.

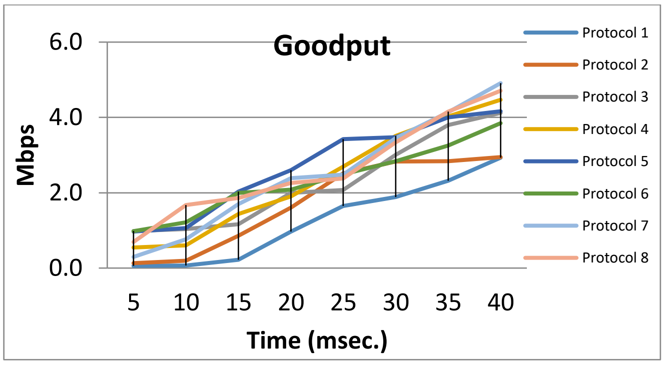

Figure 11: Comparative good analysis of ECC based authentication protocols for 200 nodes.

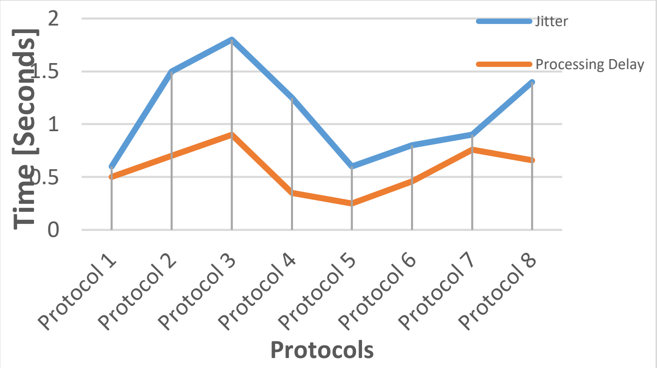

Figure 12: Comparative jitter and processing delay analysis of ECC based authentication protocols for 1000 nodes.

In performance analysis, network size is increased from 50, 75 and 100 nodes to 1000 nodes as shown in fig. 12. This experiment is conducted to analyze the performance of proposed protocols in a large network. For large network also, protocol 5 is giving better results in terms of jitter and processing delays. For large network protocol 3 is analysed to be the worst because of use of multiple cryptographic primitives. These primitives are used multiple time at each node for authenticating other devices. Protocol 7 and protocol 8 are comparatively better than protocol 2 and protocol 3 because of multi-round quick computations. Performance of protocol 1, protocol 4 and protocol 6 are comparable and better than protocol 2, protocol 3, protocol 7 and protocol 8. Thus, it is observed that use of primitives (like hashing, digital signature, message authentication codes etc.) largely affects the performance of authentication process.

V. Conclusion

In this work, 8 ECC based authentication mechanisms are analyzed for resource constrained devices. Comparative analysis of authentication protocols predicts the suitability of protocols proportionate to availability of hardware. Overall, protocol 5 is considered to be the best protocol among all others. Protocol 7 and protocol 8 are among the worst cases because of large computational cost for resource-constrained devices. Integration of lightweight cryptographic primitives in these protocols enhances the security. Performance analysis of 50 to 1000 nodes network shows that protocol 5 is best in terms of goodput, delay and jitter. A minimum of 4.3% (50 nodes network) and maximum of 12.9% (for 1000 nodes network) improvement is observed for protocol 5 as compared to other protocols. Integration of other lightweight cryptographic primitives and analysis of other QoS parameters will confirm the use of protocol 5 with least computational overhead and maximum security.

Acknowledgment

The authors would like to thank SEED Division of University of Petroleum and Energy Studies. This work is part of research project (https://sites.google.com/view/adarshproject2/) sponsored by University of Petroleum and Energy Studies (UPES), Dehradun, India under Grant: UPES/R&D/180918/14.

References

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

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

[3] J. Hoffstein, J. Pipher, and H. Joseph Silverman. "NTRU: A Ring-Based Public Key Cryptosystem". *Algorithmic Number Theory*, pp. 1-22, 1998.

[4] M. Jakobsson and S. Wetzel. "Security Weaknesses in Bluetooth". *Proceedings of the 2001 Conference on Topics in Cryptology*, pp. 176-191, 2001.

[5] CAST Inc. AES and SHA-1 Cryptoprocessor Cores. http://www.cast-inc.com. . (access on 09 April, 2019)

[6] D. J. Wheeler and R. M. Needham. "TEA :A Tiny Encryption Algorithm". Technical report, Computer Laboratory, University of Cambridge, 1995.

[7] D. J. Wheeler and R. M. Needham. "TEA Extensions". Technical report, Computer Laboratory, University of Cambridge, 1997.

[8] C. Floerkemeier and M. Lampe. "Issues with RFID Usage in Ubiquitous Computing Applications". *In Pervasive Computing (PERVASIVE)*, pp. 188–193, 2004.

[9] A. Juels. "Minimalist Cryptography for RFID Tags". *In Security in Communication Networks*, pp. 149–164, 2004.

[10] A. Juels, "Yoking Proofs for RFID Tags". *IEEE Annual Conference on Pervasive Computing and Communications Workshops, PERCOMW.2004.*1276920, 2004.

[11] A. Juels, and R. Pappu. "Squealing Euros Privacy Protection in RFID-Enabled Banknotes". *In Financial Cryptography*, pp. 103–121, 2003.

[12] A. Juels, R. L. Rivest, and M. Szydlo. "The Blocker Tag: selective blocking of RFID tags for consumer privacy". *In Proceedings of the 10th ACM conference on Computer and communication security*, pp. 103–111, 2003.

[13] D. Molnar and D. Wagner. "Privacy and Security in Library RFID : Issues, Practices, and Architectures". *Proceeding CCS '04 Proceedings of the 11th ACM conference on Computer and communications security*, pp. 210 – 219, 2004.

[14] D. Henrici and P. Muller. "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers". *Conference on Pervasive Computing and Communications Workshops*, pp. 149–153, 2004.

[15] M. Ohkubo, K. Suzuki and S. Kinoshita. "Efficient Hash-Chain Based RFID Privacy Protection Scheme". *In International Conference on Ubiquitous Computing (Ubicomp), Workshop Privacy: Current Status and Future Directions*, pp. 1-15, 2004.

[16] S. E. Sarma, S. A. Weis and D. W. Engels. "RFID Systems and Security and Privacy Implications". *In Workshop on Cryptographic Hardware and Embedded Systems*, pp. 454–470, 2002.

[17] I. Vajda and L. Buttyan. "Lightweight Authentication Protocols for Low-Cost RFID Tags". *In Fifth International Conference on Ubiquitous Computing (UBICOMP) in Seattle, Washington*, pp. 1-10, 2003.

[18] S. A. Weis, S. E. Sarma, R. L. Rivest and D. W. Engels. "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems". *In Security in Pervasive Computing* , pp. 201–212, *2004.*

[19] M. Feldhofer, S. Dominikus and J. Wolkerstorfer, "Strong Authentication for RFID Systems using the AES Algorithm". *In Cryptographic Hardware in Embedded Systems (CHES)*, pp 357-370, 2004.

[20] N. Hopper and M. Blum. "A Secure Human-Computer Authentication Scheme". *Technical report.* CMU-CS-00-139, Carnegie Mellon University, 2000.

[21] N. J. Hopper and M. Blum. "Secure Human Identification Protocols". *In Advances in Cryptology - ASIACRYPT* , pp. 52–66, *2001.*

[22] T. Matsumoto. "Human-computer Cryptography: An Attempt". *In Computer and Communi-cations Security ACM Press*, pp. 68–75, 1996.

[23] T. Matsumoto and H. Imai. "Human Identification through Insecure Channel". *In Advances in Cryptology - EUROCRYPT*, pp. 409–421, 1991.

[24] M. Naor and B. Pinkas. "Visual Authentication and Identification". *In Advances in Cryp-tology - CRYPTO,* pp. 322–336, 1997.

[25] C.-H. Wang, T. Hwang and J.-J. Tsai. "On the Matsumoto and Imai's Human Identification Scheme". *In EuroCrypt '95,* pp. 382–392, 1995.

[26] A. Juels and S. A. Weis. "Authenticating Pervasive Devices with Human Protocols". *In Advances in Cryptology – CRYPTO 2005*, pp 293-308, *2005.*

[27] S. Chari, C. Jutla, J. R. Rao, and P. Rohatgi. "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards*". In Second Advanced Encryp-tion Standard (AES) Candidate Conference, Rome, Italy*, pp. 133-147, 1999.

[28] D. Boneh, R. A. DeMillo and R. J. Lipton. "On the Importance of Checking Cryptographic Protocols for Faults". *In EUROCRYPT'97,* pp. 37–51, 1997

[29] B. S. Kaliski Jr and M. J. B. Robshaw. "Comments on Some New Attacks on Cryp-tographic Devices*". RSA Laboratories' Bulletin No. 5*, July 1997. http://www.rsasecurity.com/rsalabs/bulletins/.

[30] P. Kocher, J. Jaffe, and B. Jun. "Differential Power Analysis". *Advances in Cryptology- CRYPTO 1999*, pp. 388–397, 1999.

[31] P. C. Kocher. *Cryptanalysis of Diffie-Hellman, RSA, DSS, and other Systems Using Timing Attacks*. Technical report, Cryptography Research, Inc., 1995.

[32] H. Gobioff, S. Smith, J. D. Tygar and B. Yee. "Smart Cards in Hostile Environments". *Technical report CMU-CS-95,* In 2nd USENIX Workshop on Elec. Commerce, 1996.

[33] S. Harris, N. Shadbolt. “SPARQL query processing with conventional relational database systems”. *International conference on Web Information Systems Engineering,* pp. 235-244, 2005.

[34] A. Harth, S. Decker. “Optimized index structures for querying RDF from the web”. *Third Latin American Web Congress (LA-WEB'2005),* pp. 71-77, 2005.

[35] O. Hassanzadeh and A. Kementsietsidis. “Data Management Issues for the Semantic Web”. *IEEE 28th International Conference on Data Engineering,* pp. 1-15, 2012.

[36] J. Hayes and C. Gutierrez. “Bipartite graphs as intermediate model for RDF”. *The Semantic Web – ISWC 2004,* pp 47-61, 2004.

[37] S. R. Jeffrey, G. Alonso, M. Franklin, W. Hong and J. Widom. “A pipelined framework for online cleaning of sensor data streams”. *22nd International Conference on Data Engineering (ICDE'06),* pp. 1-10, 2006.

[38] S. R. Jeffrey, M. Garofalakis and M. J. Franklin. “Adaptive Cleaning for RFID Data Streams”, *VLDB '06 Proceedings of the 32nd international conference on Very large data bases,* pp. 163-174, 2006.

[39] S. R. Jeffrey, G. Alonso, M. Franklin, W. Hong and J. Widom. “Declarative Support for RFID Data Cleaning”, *Pervasive 2006,* pp 83-100, 2006.

[40] S. Jirka, A. Broring, C. Stasch. “Discovery Mechanisms for the Sensor Web”, *Sensors — Open Access Journal,* pp. 2661–2681, 2009.

[41] A. Juels. “Minimalist Cryptography for RFID Tags”. *International Conference on Security in Communication Networks SCN 2004,* pp. 149-164, 2004.

[42] A. Juels, R. Rivest, M. Szydlo. “The Blocker Tag: Selective Blocking of RFID tags for Consumer Privacy”. In *Proceedings ACM Conference on Computer and Communication Security,* pp. 103–111, 2003.

[43] A. Juels, J. Brainard. “Soft Blocking: Flexible Blocker Tags on the Cheap”. *Workshop on Privacy in the Electronic Society (WPES 04),* pp. 1–7, 2004.

[44] A. Juels. “RFID Security and Privacy: A Research Survey”, *IEEE Journal on Selected Areas in Communication,* XXIV (2), pp. 381–394, 2006.

[45] A. Juels, R. Pappu. “Squealing Euros: Privacy protection in RFID enabled banknotes”. In *Pro-ceedings of Financial Cryptography,* pp. 103-121, 2003.

[46] S. Kinoshita, F. Hoshino, T. Komuro, A. Fujimura, M. Ohkubo. “Low-cost RFID privacy protection scheme”, *IPS Journal,* XXXXV (8), 2004.

[47] D. Molnar, D. Wagner. *Privacy and Security in Library RFID: Issues, Practices and Archi-tectures,* In *Proceedings of the 11th ACM conference on Computer and communications security,* pp. 210-219, 2004.

[48] M. Ohkubo, K. Suzuki, S. Kinoshita. “RFID Privacy Issues and Technical Challenges”, *Communications of the ACM,* XXXXVIII (9), pp.66-71, 2005.

[49] M. Ohkubo, K. Suzuki, S. Kinoshita. “A cryptographic approach to “privacy-friendly” tags”. *RFID Privacy Workshop,* 82, 2003.

[50] S. A. Weis, S. Sarma, R. Rivest, D. Engels. “Security and privacy aspects of low-cost radio frequency identification systems”. In *Proceedings First International Conference on Security in Pervasive Computing,* pp. 201-212, 2003.

[51] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, G. Borriello. “Building the Internet of Things Using RFID”, *Journal of IEEE Internet Computing,* XXIII (3), pp. 48-55, 2009.

[52] The EPCglobal Architecture Framework, March 2009. http://www.epcglobalinc.org (Accessed: 09 April, 2019)

[53] http://seattle.intel-research.net/wisp/ (Accessed: 09 April, 2019)

[54] M. Buettner, B. Greenstein, A. Sample, J.R. Smith, D. Wetherall. “Revisiting smart dust with RFID sensor networks”. In *Proceedings of ACM HotNets,* pp. 1-6, 2008.

[55] http://www.ipso-alliance.org/ (Accessed: 09 April, 2019)

[56] B. Sterling. *Shaping Things – Mediawork Pamphlets,* The MIT Press, 2005.

[57] D. Guinard, V. Trifa. “Towards the Web of Things: Web Mashups for Embedded Devices”. In *Proceedings WWW Conference,* pp. 1-8, 2009.

[58] D. Guinard, V. Trifa, F. Mattern, E. Wilde. *From the Internet of Things to the Web of Things: Resource Oriented Architecture and Best Practices,* Architecting the Internet of Things, Springer, 2011.

[59] M-J. O. Saarinen. “The BlueJay Ultra-Lightweight Hybrid Cryptosystem”. In *Proceedings IEEE Sympo-sium on Security and Privacy Workshops,* pp. 27-32, 2012.

[60] V. S. Miller. Slide on “Elliptic Curve Cryptography: Invention and Impact: The invasion of the Number Theorists”, 2007. http://www.iacr.org/conferences/eurocrypt2007/slides/s 14t1.pdf (Accessed: 09 April, 2019)

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

[62] Juels. “RFID security and privacy: A research survey”, *IEEE Journal on Selected Areas in Communication,* XXIV (2), 381-394, 2006.

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

[64] K. Takaragi, M. Usami, R. Imura, R. Itsuki, T. Satoh, Hitachi. “An ultra small individual recognition security chip”, *Journal of IEEE Micro,* XXI (6), pp. 43-49, 2001.

[65] R. Koh, E. Schuster, I. Chackrabarti, A. Bellman. “Securing the pharmaceutical supply chain”. White Paper, Auto-ID Labs, Massachusetts Institute of Technology, pp. 1-11, 2003.

[66] M. Lehtonem, T. Staake, F. Michahelles, E. Fleisch. “From Identification to Authenti-cation- A Review of RFID Product Authentication Techniques”, In *Networked RFID Systems and Lightweight Cryptography,* P. H. Cole, D. C. Ra-nasinghe (Ed.), Springer, Berlin, Heidelberg, pp. 169-187, 2007.

[67] J. Pearson. “Securing the pharmaceutical supply chain with RFID and public key infra-structure (PKI) technologies”, Texas instruments White Paper, Available from: http://www.ti.com/rfid/docs/docntr.shtml, last accessed 2018/06/01.

[68] Z. Nochta, T. Staake, E. Fleisch. “Product Specific Security Features Based on RFID Technology”. *International Symposium on Applications and the Internet Workshops (SAINTW’06),* pp. 72-75, 2006.

[69] M. Burmester, J. Munilla. “Lightweight RFID Authentication with Forward and Backward Security”, *ACM Transactions on Information and System Security,* XIV (1), pp. 11:1-11:26, 2011.

[70] A. Kumar, K. Gopal, A. Aggarwal. “Novel Trust Hierarchical Construction for RFID Sensor-Based MANETs Using ECCs”, *ETRI Journal,* XXXVII (1), pp. 186-196, 2015.

[71] A. Kumar, K. Gopal, A. Aggarwal. “A novel lightweight key management scheme for RFID-sensor integrated hierarchical MANET based on internet of things”, *International Journal of Advanced Intelligence Paradigm,* IX (2-3), pp. 220-245, 2017.

[72] M. Lata, A. Kumar. “Survey on lightweight primitives and protocols for RFID in wire-less sensor networks”, *International Journal of Communication Networks and Information Security (IJCNIS),* VI (1), pp. 29-43, 2014.

[73] A. Kumar, A. Aggarwal. “Lightweight cryptographic primitives for mobile ad hoc networks”. In *Proceedings International Conference on Security in Computer Networks and Distributed Systems,* pp. 240-251, 2014.

[74] T. Cao, E. Bertino, H. Lei. “Security analysis of the SASI protocol”, *IEEE Transactions on Dependable and Secure Computing,* VI (1), pp. 73-77, 2009.

[75] H.-M. Sun, W. C. Ting, K.H. Wang. “On the security of Chien’s ultralightweight RFID authentication protocol”, *IEEE*

Transaction on Dependable and Secure Computing, VIII (2), pp. 315-317, 2011.

[76] P. D'Arco, A. De Santis. "On ultralightweight RFID authentication protocols", *IEEE Transaction on Dependable and Secure Computing*, VIII (4), pp. 548-563, 2011.

[77] W. Stephen, S.E. Sarma, R.L. Rivest, D.W. Engels. "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", In *Proceedings First International Conference on Security in Pervasive Computing*, pp. 201-212, 2004.

[78] A. Kumar, A. Aggarwal. "Performance analysis of MANET using elliptic curve cryp-tosystem". In *Proceedings 14th International Conference on Advanced Communication Technology (ICACT)*, pp. 201-206, 2012.

[79] A. Kumar, K. Gopal, A. Aggarwal. "Simulation and cost analysis of group authentica-tion protocols". In *Proceedings 9th International Conference on Contemporary Computing (IC3)*, pp. 1-7, 2016.

[80] A. Kumar, K. Gopal, A. Aggarwal. "A Novel and Efficient Reader-to-Reader and Tag-to-Tag Anti-Collision Protocol", *IETE Journal of Research*, XII (4), pp. 1-12, 2018. [Published Online] missing

[81] A. Kumar, K. Gopal, A. Aggarwal. "Design and Analysis of Lightweight Trust Mech-anism for Secret Data using Lightweight Cryptographic Primitives in MANETs", *Int. Journal of Net-work Security*, XVIII (1), pp. 1-18, 2016.

[82] A. Kumar, K. Gopal, A. Aggarwal, "Comparative Analysis of Elliptic Curve Cryptog-raphy based Lightweight Authentication Protocols for RFID-Sensor Integrated MANETs". In *Proceedings 18th International Conference on Intelligent Systems Design and Applications*, 2018.

Author Biographies

Dr. Adarsh Kumar received his ME degree in Software Engineering from Thapar University, Patiala, Punjab, India, in 2005 and earned his PhD degree from JIIT university, Noida, India in 2016 followed by Post-Doc from SRI, AIT, Ireleand during 2016-2018. From 2005 to 2016, he has been associated with the Department of Computer Science Engineering & Information Technology, Jaypee Institute of Information Technology, Noida, Uttar Pardesh, India, where he worked as Assistant Professor. Currently he is working with University of Petroleum & Energy Studies, Dehradun, India as Associate Professor in CSE department. His main research interests are cybersecurity, cryptography, network security, and ad-hoc networks.

Mr Saurabh Jain received his Master Degree(M.Tech) in Information Security from MANIT,Bhopal Madhya Pradesh,India in 2012,and persuing his PhD in Computer Science & Engineering from University of Petroleum and Energy Studies Dehradun, India, He has worked as an Assistant Professor in Computer Science and Engineering Department at Oriental College of Technology, Bhopal. In the past he has acted as a Head of Department in Computer Science and Engineering Department at Oriental College of Technology, Bhopal. Several other responsibilities that he has undertaken include Remote Center Coordinator of Oriental College of Technology (RC ID: 1123), a Lecturer at department of Information Technology in Bansal Institute of Science & Technology, Bhopal, and currently working as an Assistant Professor in School of Computer Science and (SoCS) at University of Petroleum & Energy Studies, Dehradun. Mr Saurabh has published 15+ research papers in reputed journals and conferences and conducted various International and national conferences, conducted multiple workshops under the mission for training of T10KT through NMEICT IIT Bombay funded by MHRD, Govt. of India. He is a certified QCSP (Quick Heal Academy Certified Cyber Security Professional) in 2018 and his research interest lies in Information, Network and web Security.

Dr. Alok Aggarwal received his bachelors' and masters' degrees in Computer Science & Engineering in 1995 and 2001 respectively and his Ph.D degree in Engineering from IIT Roorkee, Roorkee, India in 2010. He has academic experience of 18 years, industry experience of 4 years and research experience of 5 years. He has contributed more than 150 research contributions in different journals and conference proceedings. Currently he is working with University of Petroleum & Energy Studies, Dehradun, India as Professor in CSE department. His main research interests are wired/wireless networks, security, and coding theory.