Cost and Lightweight Modeling Analysis of RFID Authentication Protocols in Resource Constraint Internet of Things

Adarsh Kumar, Krishna Gopal, and Alok Aggarwal

Original scientific paper

Abstract — **Internet of Things (IoT) is a pervasive environment to interconnect the things like: smart objects, devices etc. in a structure like internet. Things can be interconnected in IoT if these are uniquely addressable and identifiable. Radio Frequency Identification (RFID) is one the important radio frequency based addressing scheme in IoT. Major security challenge in resource constraint RFID networks is how to achieve traditional CIA security i.e. Confidentiality, Integrity and Authentication. Computational and communication costs for Lightweight Mutual Authentication Protocol (LMAP), RFID mutual Authentication Protocol with Permutation (RAPP) and kazahaya authentication protocols are analyzed. These authentication protocols are modeled to analyze the delays using lightweight modeling language. Delay analysis is performed using alloy model over LMAP, RAPP and kazahaya authentication protocols where one datacenter (DC) is connected to different number of readers (1,5 or 10) with connectivity to 1, 5 or 25 tags associated with reader and its results show that for LMAP delay varies from 30-156 msec, for RAPP from 31-188 while for kazahaya from 61-374 msec. Further, performance of RFID authentication protocols is analyzed for group construction through more than one DC (1,5 or 10) with different number of readers (10, 50 or 100) and tags associated with these readers (50, 500, 1000) and results show that DC based binary tree topology with LMAP authentication protocol is having a minimum delay for 50 or 100 readers. Other authentication protocols fail to give authentication results because of large delays in the network. Thus, RAPP and Kazahaya are not suitable for scenarios where there is large amount of increase in number of tags or readers.**

Index Terms — **Authentication, Grouping, Lightweight, Modeling, RFID.**

I. INTRODUCTION

RFID systems are widely deployed in modern society. RFID technique is preferred over magnetic tapes, bar codes and smart cards due to its low cost and high speed. Due to this, its demand is continuously increasing which in turn also increasing the security risks associated with its uses. Any nearby reader can read information written on unprotected tags, trace their locations, retrieve important information, accept wrong information etc. For protecting the private information written on an unprotected tag, some mechanism is required to deter the reader from revealing the important information.

Tags are classified into authenticated and unauthenticated tags for an event in order to secure the system. Unlike unauthenticated tags, authenticated tags have strong mechanism to protect and prove their legacy. Authentication mechanisms allow a reader and a tag to protect each other by providing their authenticity. Since, RFID devices are resource constrained devices thus lightweight or ultra-lightweight mechanisms are preferred. Lightweight authentication protocols are weaker class of protocols as compared to normal authentication protocols. Lightweight pseudorandom number functions, cyclic redundancy checks (CRCs), one way lightweight hash functions at reader side etc. are allowed in lightweight authentication protocols. Ultra-lightweight authentication protocols are the weakest class of authentication protocols that uses logical bitwise operations only. RFID authentication system consists of three major tangible components: reader, tag and datacenter. Reader scans the tags for collecting required information and stores it in datacenter. These three components can prove the existence of a group through mutual authentication and grouping or yoking proofs. In mutual authentication and grouping through datacenter, each tag proves its authenticity with the reader and the reader stores the tag information in DC. DCs contain the information about each reader and tags associated with these readers. Here, reader cannot create group from identification information. It constructs groups if tags associated with products sequentially provide the information. For example, tag with identification from ‘A’ to ‘D’ are for category I product, ‘E’ to ‘G’ are for category II and so on. Now, DCs can also construct groups through two ways: (i) in a similar manner as constructed by reader or (ii) unique identification of reader and tags associated in a record stored in the DC constructs a group. Yoking proofs is another example of group authentication. In yoking proofs, multiple tags authenticate to one reader at a time. As compared to mutual authentication, subgroups can also be constructed by reader. Yoking proofs are refined form of mutual authentication that helps to construct group at lower level.

In this work, computational and communication cost analysis is performed for LMAP, RAPP and kazahaya authentication protocol. Initially this analysis is performed

Manuscript received May 15, 2014; revised July 14, 2014; revised August 16, 2014.

A. Kumar and K. Gopal are with the Jaypee Institute of Information Technology, A-10, Sector 62, Noida, Uttar Pardesh, India, Pin Code: 201307 (e-mail: adarsh.kumar@jiit.ac.in, krishna.gopal@jiit.ac.in).

A. Aggarwal is with the JP Institute of Engineering and Technology, P.O Rajpura, Meerut, Uttar Pradesh, India - 250001 (e-mail: director@jpiet.com).

1845-6421/09/8356 © 2014 CCIS

with one reader- one tag (LMAP, RAPP) or one reader-multiple tag (kazahaya). Further, authentication for long distance connectivity is proposed through DCs. Multiple DCs are interconnected through different topologies for analyzing the group formation process. Here, it is assumed that DCs contain the authentic records. Authentic stored information helps to construct and identify groups in presence of multiple DCs, readers and tags. Lightweight modeling and analysis of proposed DCs based topologies are analyzed to find the fast and economic method.

Rest of this work is organized as follows. Section II presents a critical review of mutual authentication and yoking proofs. Section III shows the notations and symbols used in this work. Section IV discusses the two mutual authentication (LMAP and RAPP) and one yoking proof (kazahaya) protocols. This section also describes the computational and communication cost analysis for these protocols. Section V proposes the group construction and cost estimation with DCs. Section VI presents the modeling and analysis of three authentication protocols using alloy model. This analysis is performed using different DCs based topologies for extending the authentication range with minimum delay. Finally the work ends up with the conclusion in section VII.

II. Related Work

Authentication protocols in cryptography can be classified into four major categories: complete, normal, lightweight and ultra-lightweight [1][2]. Ultra-lightweight authentication is the weakest class of authentication protocols. Bitwise operators (AND, OR, XOR, NOT, left shift, right shift etc.), lightweight simple pseudorandom number functions etc. are only allowed in this category. These protocols can be classified as: mutual authentication protocol and grouping or yoking-proofs protocols. Several authentication protocols are proposed for low cost RFID system [3]-[7]. Most of these protocols are prone to recording, side channel, de-synchronization, man in the middle, tracing, information leakage attacks [8][9]. In mutual authentication protocols, Lightweight Mutual Authentication Protocol (LMAP) is the first authentication protocol in ultra-lightweight authentication protocol class. Other reader to tag mutual authentication protocols are: EMAP, SASI, Gossamer, David-Prasad, HB$^+$, M2AP, RAPP etc. [10][11]. These authentication mechanisms are extended to create yoking or grouping proofs. Juels proposed the first idea of yoking that scans two tags simultaneously [12]. Several grouping protocols are proposed and analyzed in recent years [2]. Most of these protocols are prone to replay attack and uses different mechanisms to avoid this attack. These mechanisms include genetic programming, timestamping, random number etc. Kazahaya is one among of them that ensure the security guidelines required to create a group [2]. This protocol uses multiple tag and single reader authentication for creating the groups. These authentication protocols are used in various applications like: supply chain management, library management, traffic control system etc. [13]. Most of these applications face a major challenge of cost estimation in financial institutions [14]. This cost is tried to be minimum using various data center based topologies [15]. None of the earlier recent work has performed computational and communicational cost estimation of authentication protocols for data center based topologies. This work extends the data center based economic topologies to authenticate long distance placed RFID devices.

III. Symbols

The symbols used in this work are shown in table 1.

TABLE I. SYMBOLS

Symbol	Purpose
V_i	i^{th} variable
IS_{T_i}	Identification pseudonym of i^{th} tag.
ID_{T_i}/ ID_{R_i}	Identification of i^{th} tag/ reader
rn_i	i^{th} random number
$K_{T_i}^{j}$	jth key variable for ith tag
$DC_{R_i}^{k}$	Kth data center attached to ith reader.
R_i / T_i	i^{th} reader or tag

IV. Cost Analysis of Authentication Protocols

A. *LMAP*

LMAP is an ultra-lightweight mutual authentication protocol with four communications between each tag and reader [2][10]. LMAP uses simple bitwise operations: XOR, AND, OR and modulus 2^n. Tag used in this protocol requires 480 bits of rewritable memory. One identification constant (ID_{T_i}) and five key variables (four key variables ($K_{T_i}^{j}$, j∈{1,2,3,4}, i∈{1,2…n}) and one pseudonym (IS_{T_i})) with size of each of 96 bits are updated after each round of authentication. Number of rounds of authentication is dependent on number of times of reader or processes attached to reader which want to update the ID_{T_i}in database. The protocol runs as follows:

1. R_i→ T_l: {“hello”}
2. T_l→ R_i: $\{IS_{T_i}\}$
3. R_i→$DC_{R_i}^{k}$: $\{IS_{T_i}\}$
4. $DC_{R_i}^{k}$ → R_i: { $K_{T_l}^{j}$, j∈{1,2,3,4}}, $\{ID_{T_i}\}$
5. R_i→ T_l: $\{V_1 \| V_2 || V_3\}$, where $V_1 = (IS_{T_i})^{n} \oplus (K_{T_l}^{1})^{n} \oplus rn_1$, $V_2 = ((IS_{T_i})^{n} \vee (K_{T_l}^{2})^{n}) + rn_1$, $V_3 = (IS_{T_i})^{n} + (K_{T_l}^{3})^{n} + rn_2$, $(K_{T_l}^{1})^{n+1} = (K_{T_l}^{1})^{n} \oplus rn_2 \oplus ((K_{T_l}^{3})^{n} + ID_{T_i})$, $(K_{T_l}^{2})^{n+1} = (K_{T_l}^{2})^{n} \oplus rn_2 \oplus ((K_{T_l}^{4})^{n} + ID_{T_i})$, $(K_{T_l}^{3})^{n+1} = ((K_{T_l}^{3})^{n} \oplus rn_1) + ((K_{T_l}^{1})^{n} \oplus ID_{T_i})$, $(K_{T_l}^{4})^{n+1} = ((K_{T_l}^{4})^{n} \oplus rn_1) + ((K_{T_l}^{2})^{n} \oplus ID_{T_i})$ and $(IS_{T_i})^{n+1} = (IS_{T_i})^{n} + (rn_2 \oplus (K_{T_l}^{4})^{n}) \oplus ID_{T_i}$.
6. T_l→ R_i: $\{V_4\}$, where $V_4 = ((IS_{T_i})^{n} + ID_{T_i}) \oplus rn_1 \oplus rn_2$. Here, T_l extracts rn_1, verify $V_2$and generate V_4.
7. R_i: Verify $\{V_4\}$.

Table II and III show the computational and communication cost of single run in one reader, one tag and one DC for LMAP in n-rounds. Results show that computational cost of tag is higher than reader and communication cost of reader is higher than tag. Since multiple tags are attached to one reader thus overall computational and communication cost of reader is much higher than single tag cost.

TABLE II. COMPUTATIONAL COST IN LMAP

Parameter	Reader Cost	Tag Cost
Number of bitwise-XOR operations	12n	18n
Number of bitwise- OR operations	n	n
Number of Addition (mod 2^n) operations	8n	9n
Number of Constant stored	_	1
Variable updating cost	105n	140n

TABLE III. COMMUNICATION COST IN LMAP

Parameter	Reader Cost	Tag Cost
Number of messages	3n+2	2n
Size of message (sent)	(328n+96) bits	192n bits
Size of message (received)	(192n+480) bits	328n

B. *RAPP*

RAPP is an ultralightweight mutual authentication protocol to avoid de-synchronization attack [11]. This protocol is different from existing authentication protocols because of permutation operations. It uses data permutation rather than logic bitwise operations. RAPP protocol runs as follows:

1. $R_i \rightarrow T_l$: {“hello”}
2. $T_l \rightarrow R_i$: $\{IS_{T_i}\}$
3. $R_i \rightarrow DC^k_{R_i}$: $\{IS_{T_i}\}$
4. $DC^k_{R_i} \rightarrow R_i$: { $K^j_{T_l}$, j$\epsilon$$\{1,2,3\}$}, $\{ID_{T_i}\}$
5. $R_i \rightarrow T_l$: $\{V_1 \| V_2\}$, where V_1=Permutation(($(K^2_{T_l})^n$, $(K^1_{T_l})^n$) $\oplus$ rn_1, V_2= Permutation((($(K^1_{T_l})^n \oplus (K^2_{T_l})^n$), Rot ($rn_1$, rn_1)) $\oplus$ Permutation($rn_1, K^1_{T_l}$), $(K^1_{T_l})^{n+1}$ =Permutation ($(K^1_{T_l})^n$, rn_1) $\oplus$$(K^2_{T_l})^n$), $(K^2_{T_l})^{n+1}$ =Permutation ($(K^2_{T_l})^n$, rn_1) $\oplus$$(K^1_{T_l})^n$), $(K^3_{T_l})^{n+1}$ = Permutation(($(K^3_{T_l})^n$, ($rn_1 \oplus rn_2$)) $\oplus$ $(IS_{T_i})^n$) and $(IS_{T_i})^{n+1}$= Permutation (($(IS_{T_i})^n$, ($rn_1 \oplus rn_2$)) $\oplus$ $(K^1_{T_l})^n \oplus (K^2_{T_l})^n \oplus (K^3_{T_l})^n$.
6. $T_l \rightarrow R_i$: $\{V_3\}$, V_3= Permutation (($rn_1 \oplus (K^1_{T_l})$, ($rn_1 \oplus (K^3_{T_l}) \oplus ID_{T_i}$.
7. $R_i \rightarrow T_l$: $\{V_4, V_5\}$, V_4= Permutation(($(K^3_{T_l})^n$, $(K^2_{T_l})^n$) $\oplus$ rn_2, V_5= Permutation(($(K^3_{T_l})^n$, Rot(rn_2, rn_2)) $\oplus$Permutation(rn_1, $(K^3_{T_l})^n \oplus (K^2_{T_l})^n$).

Table IV and V show the computational and communicational cost of single run in one reader, one tag and one DC for RAPP in n-rounds. Results show that computational and communication cost of tag is lesser than reader. The cost of computational and communication for reader increases at higher rate than tag with increase in number of tags attached to reader.

TABLE IV. COMPUTATIONAL COST IN RAPP

Parameter	Reader Cost	Tag Cost
Number of bitwise-XOR operations	16n	14n
Number of bitwise- Shift operations	192n	-
Number of Permutation Operations	16n	7n
Number of Constant stored	-	1
Variable updating cost	224n	21n

TABLE V. COMMUNICATION COST IN RAPP

Parameter	Reader Cost	Tag Cost
Number of messages	5n	2n
Size of message (sent)	(424n + 96) bits	192n bits
Size of message (received)	(192n + 384n) bits	424n

C. *Kazahaya: An RFID Grouping Protocol for Low-Cost RFID Tags*

Peris *et. al.* proposed Kazahaya protocol for groups with special interest [2]. Each group has a unique identification number and group key. Datacenter attached to reader stores the identification marks of tags in a group to identify the groups. Kazahaya is designed to meet the security requirements for authentication protocols and it runs as follows:

1 $R_i \rightarrow T_l$: {TS_n}, where TS_n is the timestamp.

2 $T_l \rightarrow R_i$: {$rn^{T_l}_1$, $rn^{T_l}_2$, I^1_{group}, $I^2_{T_l}$ }, where $rn^{T_l}_1$ and $rn^{T_l}_2$are two random number generated by T_a. I^1_{group}= PRNG ($ID_{group} \oplus rn^{T_l}_2 \oplus PRNG(K_{group}) \oplus$ PRNG (TS_n)). $I^2_{T_a}$ = PRNG($ID_{T_l} \oplus rn^{T_l}_1 \oplus$ PRNG(K_{T_l}) $\oplus$PRNG(TS_n+1)). Here, K_{group} is the group key, I^1_{group} and $I_{T_a}$are the temporary variables.

3 $R_i \rightarrow T_m$: {TS_n, $rn^{T_l}_2$, I^1_{group}, I_{T_l} }. Reader store $rn^{T_l}_1$.

4 T_m verifies I^1_{group} equals PRNG ($ID_{group} \oplus rn^{T_l}_2 \oplus PRNG(K_{group}) \oplus$ PRNG (TS_n)). If it equals then it generate two random numbers: $rn^{T_m}_1$ and $rn^{T_m}_2$, and computes I^2_{group}= PRNG ($ID_{group} \oplus rn^{T_m}_2 \oplus PRNG(I^1_{group})$. $I^2_{T_m}$ = PRNG($ID_{T_m} \oplus rn^{T_m}_1 \oplus$ PRNG(K_{T_m}) $\oplus$PRNG($I^2_{T_l}$)).

$T_m \rightarrow R_i$: { $rn^{T_m}_2$, $rn^{T_m}_1$, I^2_{group}, $I^2_{T_m}$ }

5 $R_i \rightarrow T_l$: { $rn^{T_m}_2$, I^2_{group}, $I^2_{T_m}$ }. R_i stores $rn^{T_m}_1$.

6 T_l verifies I^2_{group} equals PRNG ($ID_{group} \oplus rn^{T_m}_2 \oplus PRNG(K_{group}) \oplus$ PRNG (I^1_{group})). If it equals then it

computes $I_{T_{lm}}$ =PRNG($ID_{T_l} \oplus I_{T_l}^2 \oplus$ PRNG($I_{T_m}^2$) ⊕ PRNG(K_{T_l}+1)).

$T_l \rightarrow R_i$: $\{I_{T_{lm}}\}$

7 R_i generate evidence $e_n^{T_{lm}}$= $\{ID_{T_l}$, ID_{T_m}, TS$_n$, $rn_1^{T_l}$, $rn_1^{T_m}$, $I_{T_{lm}}\}$

Table VI and VII show the computational and communicational cost of single run in one reader, two tags and one DC for Kazahaya authentication protocol in n-rounds. Results show that computational cost of reader is negligible as compared to group tag cost whereas communication cost of reader is higher than any individual tag cost. Computational cost of first tag is higher than second tag and communication cost of first tag is double the cost of second tag.

TABLE VI. COMPUTATIONAL COST IN KAZAHAYA

Parameter	Reader Cost	First Tag Cost (T_l)	Second Tag Cost (T_m)
Number of bitwise-XOR operations	-	12n	9n
Number of bitwise-PRNG operations	-	12n	9n
Number of Addition Operations	-	2n	-
Number of Variable stored	2n	-	-
Variable updating cost	-	4n	3n

TABLE VII. COMMUNICATION COST IN KAZAHAYA

Parameter	Reader Cost	First Tag Cost (T_l)	Second Tag Cost (T_m)
Number of messages	8n	4n	2n
Number of messages (sent)	4n	2n	n
Number of messages (received)	3n	2n	n

V. COST ANALYSIS OF LONG RANGE GROUP AUTHENTICATION

Figure 1 shows an example where 4 DCs are connected in a *circular topology*, 3 readers are connected with each DC and each reader can scan 3 tags simultaneously. Similarly, more DCs can be connected and tags are considered to be authentic if DC contains the record of respective tags. DCs communicate in circular topology for synchronizing the tag records. Tag record packet comes back to original resource after updating the data in every DC and gives acknowledgement that record has been updated in every DC. This approach can be extended for more number of RFID devices including data centers. Reader cost of computation increases with increase in number of tags attached to it. Similarly, data centers cost also increases with increase in readers attached to it. In computational cost, nearby DC stores 5 variables and 1 constant for LMAP, 4 variables and 1 constant for RAPP, and 2 variables and 1 constant for kazahaya authentication protocol. Variables in LMAP and RAPP are updated once in n-rounds whereas these are updated n-times in n-rounds for kazahaya. For calculating communication cost, tag-reader mutual authentication communication cost is added to DC communication cost. Various designs of scanning the tags by readers, attachments of DCs to readers and integration of DCs are followed to: improve the centralized or distributed network control, reduce the computational or communication cost, enhance the network performance and increase the availability of data. These DCs are connected in various other ways: (i) peer to peer, (ii) centralized or (iii) semi–decentralized / semi-centralized.

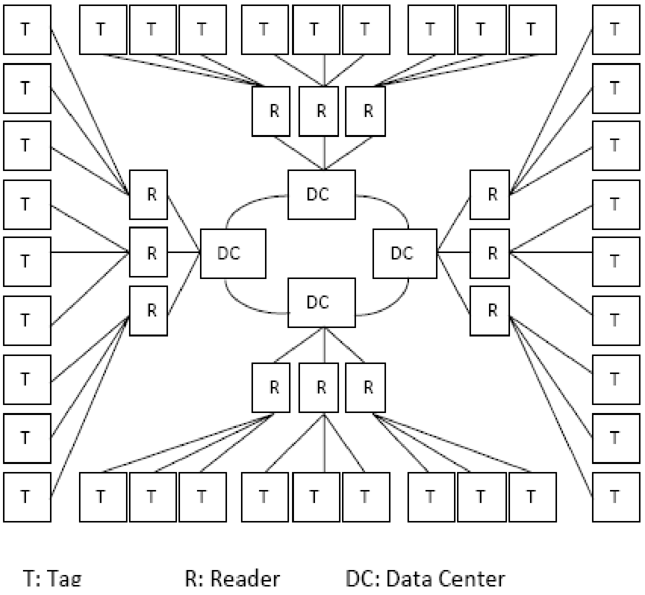

Figure 1: 3T-3R-4DC Design (with DC as in circular topology).

In *peer to peer connectivity*, any DC can establish connection with any other DC in one to one manner. Synchronization of DCs is necessary to ease the availability of data. This synchronization occurs in proactive or reactive manner. Proactive data updating procedure stores the data at local DCs prior to any request. This may follow a time clock to synchronize and update the data. In reactive procedure, whenever there is need to access the data then a new connection is established to synchronize the required data. In proactive case, 'n-1' communications are required to update the records. In reactive case, if 'b'-bunch of requests are updated simultaneously then floor((n-1)/b) communications are required. Figure 2 shows pseudo-code of updating the DC records in peer to peer connection. This approach avoids the drawback of central point failure. This is a good approach for file sharing in a small network. IoT in close vicinity allows the file sharing at much faster rate compared to centralized or circular approach.

```
for i=1 to m-1:
    for j=i+1 to m:
        DC[i]→DC[j]: Exchange($IS_{T_i}$, $ID_{T_l}$, Keys)
    end
end
```

Figure 2: DC design with peer to peer connectivity.

```
for i=1 to m-1:
    if local LMDC exist then :
        DC[i]→LMDC: Exchange($IS_{T_i}$, $ID_{T_i}$, Keys)
            If more LMDC exist then:
                LMDC→Next(LMDC): ($IS_{T_i}$, $ID_{T_i}$, Keys)
            else
                continue
    else:
        LMDC→MDC: Exchange($IS_{T_i}$, $ID_{T_i}$, Keys)
end
```

Figure 3: DC design with centralized Master Data Center (MDC)

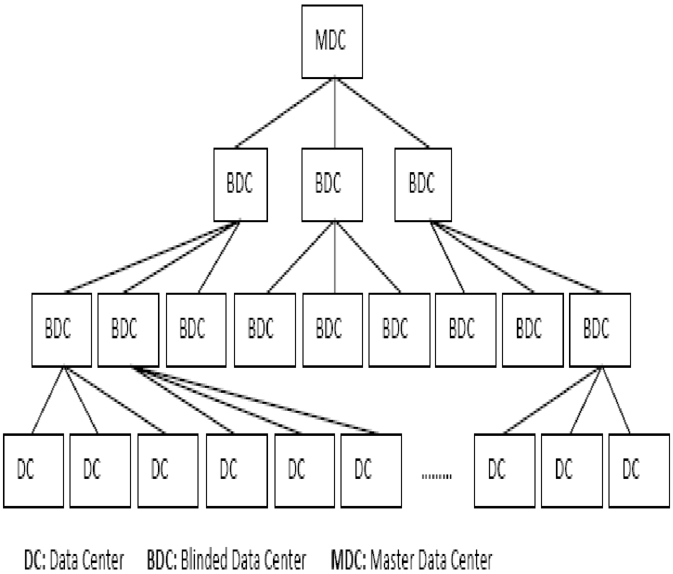

Figure 4: 3-ary tree design for data centers

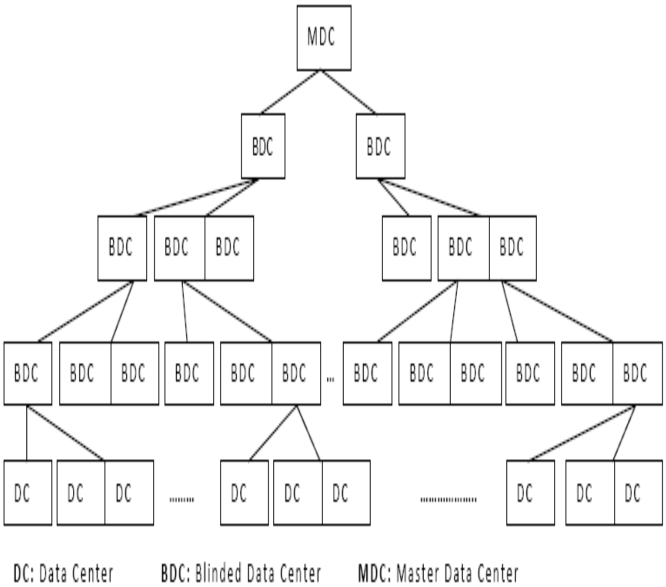

Figure 5: (2-3)- ary tree design for data centers

TABLE VIII. COMMUNICATION COMPLEXITY

Circular	$O(n^2)$
Centralized	$O(\log_n n)$
Peer to Peer	$O(n^2)$
k-Tree	$O(\log_n n)$
n-m Tree	$O(\log_n n)$

In *centralized connectivity*, a central master DC (MDC) is maintained that updates the records from local DCs or local MDCs (LMDC). Here, DCs are connected to LMDC or MDC. There may be multiple LMDCs in the path. Figure 3 shows the pseudo-code of updating the MDC from DCs. These records update are processed either to direct connection between DC and MDC or DC to multiple LMDC and then finally with MDC. Cost of communication increases with each connection. If DC is ‘r’ connections away from MDC then 6r variables and one constant updates per record are required for LMAP. For RAPP, this cost reduces to 5r variables and one constant. This cost is 4r variables and two constants for kazahaya. However, this cost can be minimized if multiple records are updated at same time in any DC.

K-ary tree construction method is another centralized mechanism that improves the communication cost and provides multiple centralized points to update the records. Figure 4 shows an example of 3-ary centralized tree construction. There are multiple BDCs that are central points to manage the records and do not interact directly with the readers. In worst case, if n-tags are attached to single reader, n-readers to single DC, n-DCs to single BDC and n-BDCs to single MDC then cost of updating all the records is $n\log_n n$. This approach is preferred if BDCs are placed a distance apart but if some BDCs are closely connected then (n-m)-tree construction is preferable. Figure 5 shows an example of (2-3)-ary tree construction. In worst case, if ‘n’ tags are connected to single reader, n-readers to single DC, m-DC to single BDC and m-BDC to single BDC in its parent layer then cost of updating all the records is less than $n\log_n n$.

Table VIII shows the comparative analysis of communication complexities. It shows that centralized mechanisms are having better communication complexities compared to circular or peer to peer connectivity. A centralized mechanism provides better resistance to attacks compared to de-centralized mechanism. These communication complexities are same for searching, inserting and deleting a new data record in DCs. The proposed approaches of constructing large RFID network group deployment is better in terms of security, extendibility and design simplicity compared to existing distributed or proximity based network topology construction using genetic algorithms [16][17]. Distributed designs have limited scalability and performance of network decreases with fixed approach to transfer data and construct groups [16]. Security, scalability and performance of networks are extended with increase in data centers and their connectivity in proposed techniques. There is increase in security because the use of authentication protocols enhances the valid users to take part in data transfer. Here, performance of network is not affected because large part of communication cost for data exchange is bearded by data centers and their connectivity. These data centers reduce the use of other hardware devices in the networks. Zhao *et. al.* design use switches, routers and other network devices to transfer the data [16]. A dedicated network design in this approach reduces the security of network because same link is used for a long time to transfer the data. However, the techniques proposed in this work estimate the proximity of devices to transfer the data in an authenticated way. Genetic algorithm based network design also use proximity of RFID devices to exchange information [17]. But this approach is good for short range connectivity. More RFID network designs are required to extend the possibility of information availability. Thus, proposed current work is better than existing approaches to exchange information and construct long range information availability groups. This is important for various applications especially IoT.

VI. Modeling and Analysis

The proposed group schemes are tested for low cost passive RFID EM4100 family transponder tags. Reader has the reading distance of 10-15 centimeters at 125 KHz reading frequency. Transponder tag contains unique identifier selected from billions of possible combinations. Reader reads this identifier and transmits to data centre server via a simple serial interface. Tag identifier works with 64-bits data stream which includes header, identification, data and parity bits. Alloy language and model is used for modeling and testing the protocols. Results obtained after modeling is important for designing applications in various domains like: household security devices, position locating and tracking services, data sharing applications, medicating the patients in healthcare systems, supply chain management, etc. Result data is quantitatively important to design more efficient applications with group construction methods.

In modeling of lightweight authentication protocol, reader, tags and DCs are kept as independent entities. Reader scans the tags. Identification pseudonyms, identification constant, and keys are stored in datacenters. Figure 6 shows a LMAP alloy model for single reader and single tag authentication [18]. After sending *IS* to reader, datacenter generates the keys and forwards these to reader. Reader receives keys and tag identification for generating next message. Table IX shows the delay analysis when protocols are analyzed using alloy model. Results show that LMAP protocol is having minimum delay compared to RAPP or kazahaya. Three different scenarios are taken into consideration with variations in readers and tags. In first scenario, one datacenter is connected to one reader and 1, 5 or 25 tags. Readers are increased to 5 with connectivity of 1, 5 or 25 tags to each reader in second scenario. Numbers of readers are further increases to 10 with 1, 5 or 50 tags to each reader in third scenario. Results show that delay in RAPP or LMAP is half of Kazahaya in worst scenarios. Increase in delay is because of increase in tags rather than increase in readers. When readers are increased then delay decreases because more devices are available to handle tags. Here, parallel operations reduce the delays. However, when ratio of number of tags to number of readers increases then delays also increases. This increase is highest for kazahaya and lowest for LMAP.

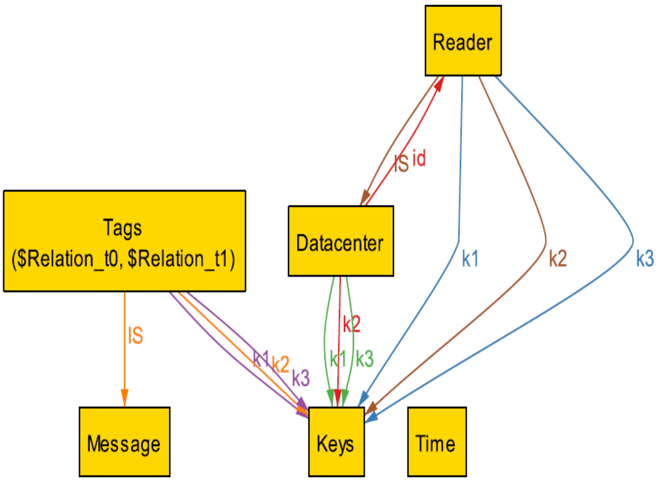

Figure 6: LMAP model for single reader-single tag authentication.

TABLE IX. Delay Analysis for different number of Readers and Tags associated with Readers.

Readers	Tags	Time [msec]		
		LMAP	RAPP	Kazahaya
1	1	30	31	61
1	5	62	70	112
1	25	94	97	131
5	5	32	47	86
5	25	62	76	113
5	125	96	102	144
10	10	40	31	87
10	50	94	104	156
10	500	156	188	374

DC0
update
DC1
update
DC2
update
DC3
update

Figure 7a: 4-Data Centers update their records from Readers and Tags

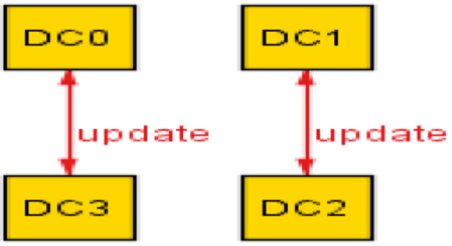

Figure 7b: Data Centers exchange records in parallel.

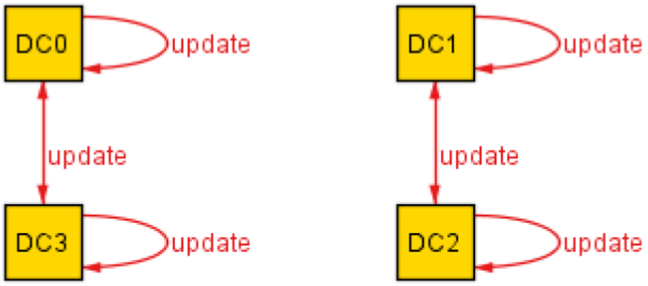

Figure 7c: Each Data Center Update its records.

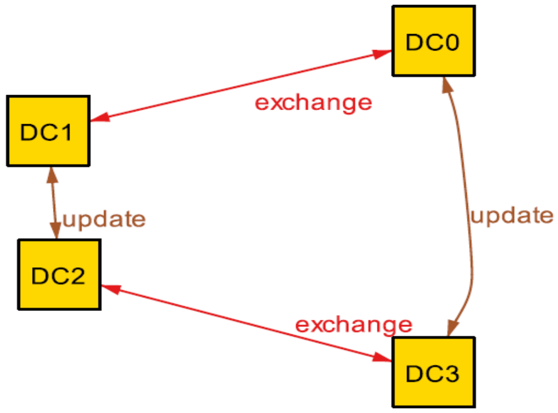

Figure 7d: Data Centers update their records in circular connectivity.

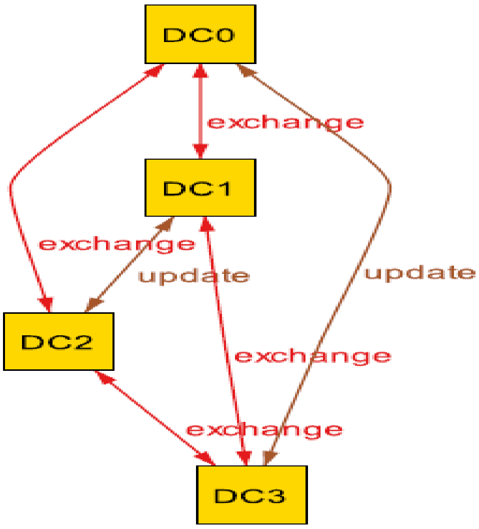

Figure 7e: Each Data Centers update records with other data centers in peer to peer connectivity.

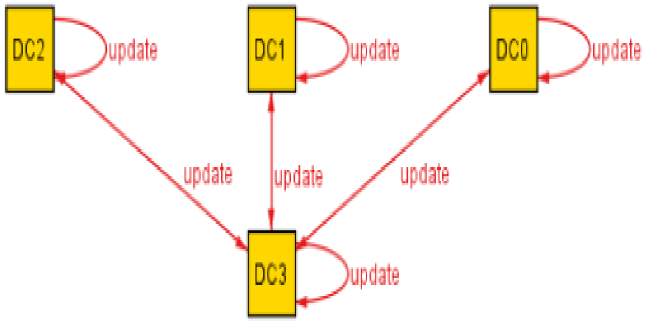

Figure 7f: Data Centers update their records in Centralized MDC connectivity.

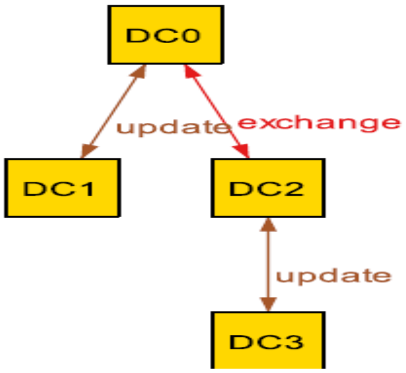

Figure 7g: Data Centers update their records in Tree (k=2) connectivity.

Figures 7a to 7g show an example how 4 DCs update their records through different topologies. Figure 7a shows an example how four DCs update their records from readers that are connected to tags. DCs exchange their records in parallel to synchronize the data after fetching records from readers. Figure 7b shows how a pair of DCs exchanges the data in parallel. Once data is exchanged then each DC matches the received data with stored data to update its records as shown in figure 7c. Now, DCs can update their records using circular, peer to peer or centralized topology. Figure 7d shows an example how four DCs exchange and update their records in curricular process. Any two nearby DCs can exchange and update their information in circular topology. It is bidirectional and exchange or update is possible simultaneously. Figure 7c shows the exchange and updating process of DC0 with DC3 and DC1 with DC2. Figure 7d shows the exchange process of DC0 with DC1 and DC2 with DC3. Alloy analysis also shows the possibility of data updation between DC0 with DC3 and DC1 with DC2. Figure 7e shows the record exchange and update process in peer to peer connectivity. Here, each DC updates its record with every other DC. Figure 7f shows an example of centralized star connectivity. In this example, DC3 is acting as master centralized DC, i.e. MDC and all other DCs update their records through single MDC (i.e. DC3). Communication overhead for DC3 in this topology is highest among all. Updating process with sequence number 1 is processed first then process with sequence number 2 is executed to update the records. This record updation is also possible through tree topology as shows in figure 7g. DC3 is child DC of DC2, and DC1 and DC2 are child DC of DC0. Each child DC updates its record with its parent DC. DCs create tree with fixed or variable number of child DCs. Examples of fixed number of child are: uniary (serial, k=1), binary (k=2), ternary (k=3), quaternion (k=4) and so on. Variable numbers of DCs examples are: (n-m)-ary tree, (n-m-o)-ary tree, R-tree, X-tree etc.

TABLE X. DELAY ANALYSIS FOR DIFFERENT NUMBER OF DCS, READERS AND TAGS FOR VARIOUS TOPOLOGIES.

Data Centers	Readers	Tags	Time [msec]		
			LMAP	RAPP	Kazahaya
Circular Topology					
1	10	50	94	104	156

5	50	500	274	312	441
10	100	1000	543	timeout	timeout
Peer to Peer Connectivity					
1	10	50	94	104	156
5	50	500	345	413	653
10	100	1000	651	timeout	timeout
Centralized MDC Connectivity					
1	10	50	94	104	156
5	50	500	378	410	534
10	100	1000	614	917	1123
K-ary tree connectivity (with k=2)					
1	10	50	94	104	156
5	50	500	238	319	450
10	100	1000	489	875	1031
(2-3)-ary Tree Connectivity					
1	10	50	94	104	156
5	50	500	316	367	511
10	100	1000	553	890	1092

Table X shows the delay analysis with increase in readers, tags or DCs, or connectivity of multiple DCs through different topologies. Two de-centralized (circular and peer to peer) and three centralized (central MDC, K-ary tree and (2-3)-ary tree connectivity) approaches are considered for delay analysis. Results show that when single DC is considered for storage with 10 readers and 50 tags then delay is least. This is because data storage is occurring parallel to reader-tag authentication operations. Delay increases with increase in DCs or increase in reader and tags connected with these DCs. Centralized approaches consume less delay compared to de-centralized approaches with increase in DCs, readers or tags. Increase in delay is minimum for K-ary tree (with k=2) and maximum for peer to peer connectivity. When readers and tags are increased to a large number then it becomes almost impossible for centralized mechanism to synchronize the data records within a stipulated time. However, if delays are not important then it is possible to synchronize the data records with maximum fault tolerance in large networks for RAPP and kazahaya protocols using de-centralized mechanisms. Overall, LMAP is found to have minimum delay among centralized or de-centralized approaches compared to other protocols. Delay comparison with existing techniques shows that the proposed mechanisms are having less delay and its variations. A variation of less than 1/100 msec. is observed as compare to other similar techniques [19].

VII. Conclusion

In this work, two mutual and one yoking proof authentication protocols are extended to construct long range groups. This work is an extension to cost-benefit analysis using authentication protocols in DCs [15]. Here, groups are constructed through DCs. DCs follow different topology to update their records and extend the information availability. This information also extends the authenticity of tags in a large group. Further, DC connectivity is analyzed through lightweight modeling language to estimate the delays in construction of different DCs based connectivity models. Among three protocols (LMAP, RAPP and kazahaya), LMAP has shown the minimum delay for one reader and attachment of multiple tags (maximum tags = 50). De-centralized DC topologies are better compared to centralize for small scale authentication through DCs. A maximum of 651 msec. delay is observed in de-centralized peer to peer connectivity as compared to 614 msec. in centralized MDC connectivity using LMAP protocol. Results show that there are large delays using RAPP and Kazahaya for centralized topologies compared to de-centralized topologies for large scale networks. These tests are valid for passive devices that support the lightweight authentication protocol.

References

[1] H. Y. Chien, “SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity,” *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 4, pp. 337-340, 2007.

[2] P. Peris-Lopez, A. Orla, J. C. Hernandez-Castro, and J. C. Lubbe, “Flaws on RFID grouping-proofs. Guidelines for future sound protocols,” *Journal of Network and Computer Applications*, vol. 34, no. 3, pp. 833-845, 2011.

[3] C. Su, Y. Li, Y. Zhao, R. H. Deng, Y. Zhao and J. Zhou, “A Survey on Privacy Frameworks for RFID Authentication,” *IEICE Transactions on Information and Systems*, vol. E95-D, no. 1, pp. 2-11, 2014.

[4] M. Langheinrich, “A Survey of RFID Privacy Approaches,” *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 413-421, August 2009.

[5] Y. Uousuf, V. Potdar, “A Survey of RFID Authentication Protocols,” *22^{nd} International Conference on Advanced Information Networking and Applications*- Workshops, Okinawa, March 2008, pp. 1346-1350.

[6] I. Syamsuddina, T. Dillonb, E. Change and S. Hand, “A Survey of RFID Authentication Protocols Based on Hash-Chain Method,” *3^{rd} 2008 International conference on convergence and hybrid information technology*, Busan, South Korea, Nov. 2008, pp. 559-564.

[7] P. Dusart and S. Traor, “ Lightweight Authentication Protocol for Low-cost RFID Tags”, *WISTP 2013*, 2013, pp. 129-144.

[8] T. van Deursen and S. Radomirovic, “Attacks on RFID Protocols,” *IACR Cryptology ePrint Archive Report*, 2008/310. http://eprint.iacr.org/2008/310.pdf

[9] Peris-Lopez, P., Li, T., Lim, T.-L., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., and Ribagorda, A.,“Cryptanalysis of a novel authentication protocol conforming to EPC-C-1G-2 standard,” *Computer Standards & Interfaces*, vol. 31, no. 2, Feb. 2009, pp. 372-380.

[10] H. Y. Chien, “The Study of RFID Authentication Protocols and Security of Some Popular RFID Tags,” in *Development and Implementation of RFID Technology*, I-Tech Education and Publishing, 2009, pp. 261-291.

[11] Z. Ahmadian, M. Salmasizadeh, and M. Reza Aref, “Desynchronization Attack on RAPP Ultralightweight Authhentication Protocol,” *Information Processing Letters*, vol. 113, no. 7, pp. 206-209, April 2013.

[12] A. Juels, “Yoking-Proofs for RFID Tags,” *International Workshop on Pervasive Computing and Communication Security- PerSec 2004*, IEEE Computer Society, Orlando, Florida, USA, 2004, pp. 138-143.

[13] C. C. Aggarwal, J. Han, “A Survey of RFID Data Processing,” *Managing and Mining Sensor Data* 2013, 2013, pp. 349-382.

[14] V. Avelar,”Data Center Physical Infrastructure for Radio Frequency Identification (RFID) systems,” White Paper 89, pp. 1-10, Revision 1. http://www.apc-by-schneider-electric.de/whitepapers.php?t=White%20Papers&m=whitepapers

[15] N. A. Khan, R. Vaverde,"The Use of RFID Based Supply Chain Systems in Data Centers for the Improvement of the Performance of Financial Institutions," *Engineering Management Research*, vol. 3, no. 1, pp. 24-35, 2014.

[16] Y. Z. Zhao, O. P. Gan, "Distributed Design of RFID Network for Large-Scale RFID Deployment", *IEEE International Conference on Industrial Informatics*, Singapore, 16-18 August 2006, pp. 44-49.

[17] O. Botero, H. Chaouchi, "RFID network topology design based on Genetic Algorithms", *IEEE International Conference on RFID-Technologies and Applications (RFID-TA)*, Sitges, 15-16 September 2011, pp. 300-305.

[18] Alloy Analysis: http://alloy.mit.edu/alloy/

[19] I. Paparrizos, S. Basagiannis, S. Petrodou, "Quantitative Analysis fir Authentication of Low-cost RFID Tags", *IEEE Conference on Local Computer Networks,Bonn, Germany*, Oct. 2011, pp. 295-298.

Adarsh Kumar is currently working as Assistant Professor in Computer Science Engineering and Information Technology department at Jaypee Institute of Information Technology, Noida, INDIA, since September 2005. Mr. Kumar received his B.Tech (Computer Science) and M.Tech (Software Engineering) from Punjab Technical University and Thapar University, Patiala in June 2003 and July 2005 respectively. He is pursuing PhD in Computer Science from Jaypee Insttute of Information Technology, Noida, INDIA.

Krishna Gopal is currently working as Dean (Academic and Research) at JIIT, Noida, INDIA since 2011. He is having 45 y ears of teaching and R&D experience. He received his Bachelor, Master and PhD in Electronics engineering from IIT, Madras, REC Kurukshetra in 1966, 1972, 1979 respectively. He published more than 100 papers in different journals, conferences, patents etc. He has done various administrative responsibilities like: Director, Dean in REC Kurukshetra. He is member of various professional bodies like: Life Member System Society of India, Indian Society for Technical Education, Senior member of IEEE etc.

Alok Aggarwal is currently working as Professor and Director at JP Institute of Engineering and Technology, Meerut, INDIA, since 2012. He is having work experience of sixteen years with a mix of software developer, research and teaching. He received his Bachelor, Master and PhD in Computer Science and Engineering from Kurukshetra University and IIT, Roorkee in 1995, 2001, 2010 respectively. He published four books and more than hundred research papers in different journals, conference proceedings etc.