Comparison of various Security Protocols in RFID

Vaibhaw Dixit
Department of Computer Science and Engineering, Dr B R Ambedkar National Institute of Technology, Jalandhar, Punjab, India

Harsh K. Verma
Department of Computer Science and Engineering, Dr B R Ambedkar National Institute of Technology, Jalandhar Punjab, India

Akhil K. Singh
Department of Computer Science and Engineering, Dr B R Ambedkar National Institute of Technology, Jalandhar Punjab, India

ABSTRACT
Paper presents a brief overview of RFID technology and protocols used in it. The paper becomes a foot step in analysis and contrasting Kill Tag, Hash-Lock, Enhanced Hash Lock, Selective Blocker Tag, Tag Broker Model and Molnar Wagner controlled delegation on the basis of security, implementation cost and practical implementation possibility. The discussion results in a selection of protocol as per the requirement and environment of use.

Keywords
RFID, Kill Tag, Hash-Lock, Enhanced Hash Lock, Selective Blocker Tag, Tag Broker Model and Molnar Wagner Controlled Delegation

1. INTRODUCTION
Radio systems have gained immense popularity during recent years. The motivation behind the pervasive use of RFID systems is the need to fully automate remote tracking and identification of objects by embedding cheap and low power RFID tags in the objects. RFID tags are composed of an antenna and a small microchip with some identification information encoded in it the data transmitted by the tag may contain identification or location information or specifies about the product being tagged, such as price colour, date of purchase etc. The RFID technology is rife with problems related to security and privacy. There is concerns that information stored on RFID tags could be read by anyone with an RFID reader – data thieves hackers, or forgers. In such a setup, the RFID system is exposed to a number of security attacks [1, 2] and privacy issues. Possible security attacks and privacy issues are outlined below:

1.1 Security attacks
Eavesdropping the adversary can monitor the wireless unsecured communication easily and collect the information transmitted by tag.

Spoofing refers to imitating the behavior of a genuine label. An adversary may replace a valid item with a fake tag or replace the tag of an expensive item with that of a fake tag with data obtained from a cheaper item.

Denial of Service An adversary may initiate a Denial of Service attack (DOS) to bypass or avoid Security systems. A DOS attack is easily carried out by placing a large number of fake tags for identification by a reader. He may also have the ability to disrupt an RFID system implementation by destroying or corrupting a large batch of tags. Such brute force attack raise concerns regarding system availability.

Tampering Another avenue for attacking an RFID security mechanism might be a physical attack on an RFID tag or a reader to discover the information stored in tag.

Man in the middle attack an adversary can modify the response of the tag to the reader. Traffic Analysis Monitoring of communication between reader and tag allows adversary to perform traffic analysis and generate statistical data.

Replay Attack The attackers can eavesdrop the response message from the tag, and retransmit the message to the legitimate reader.

Data loss the protocol can be damaged by power interruption, hijacking, and database desynchronization.

1.2 Privacy issues
The RFID privacy problem has two components [3]. The first one concerns the leakage of information about user belongings, and the second one is related to tracking and identification by forming associations between tags and their holders. The two aspects are explained below:

Information Leakage In the absence of confidentiality and authentication mechanism, there is a possibility for unauthorized readers to gain access to tag information, which is a threat to user privacy. For example, banknotes labeled with RFID tags may reveal the cash balance of a person. Also, this also involves the risk of corporate espionage, as lack of proper access control enables monitoring of competitor's inventory.

Behavioral Tracking [4] and personal identification another important privacy concern is the tracking of individuals by RFID tags carried by them. Also, if the consumer buys an item using a credit card and an adversary can link the credit card details with that of purchased tagged item, the identity and movements of the consumer can be traced. Correlating data from multiple tag reader locations, adversary could track movement, social interactions, and financial transactions of the user. Even if the tags are protected, i.e. they only contain product codes rather than unique serial numbers, individuals could still be tracked by the constellation of products they carry.

2. PROTOCOLS DISSCUSION
2.1 Tag Broker Model
In Tag broker model, a tag broker (i.e. third party) is merged in present RFID environment to improve security and privacy of RFID system. Tag broker basically generates tag pseudonym for product manufactures and it has translation rules for generating original tag values from tag pseudonym on query by tag reader.

Product manufacture manages original tag values and its related content providers. Fig.1 shows Tag broker model, merged in mobile RFID service architecture.
Working of Tag broker model:

1) Tag broker generates tag pseudonym for product manufactures to attach to their product.
2) RFID readers detects tag pseudonym and want to get item information .to get item information reader contacts to ONS(object name server) which gave address of tag broker.
3) RFID reader transmit tag pseudonym to tag broker which translate it to original value .tag broker then request item information from content provider using original tag value.
4) Content provider returns item information which is permitted to user to tag broker and tag broker transmit this information to RFID reader.
5) Tag broker returns the response. Of course, user cannot find out original tag value from tag pseudonym in this scenario.

Tag pseudonym

Tag pseudonym should be random such that no one without tag broker can find original tag value from the tag pseudonym. Formation of tag pseudonym is shown below:
Tag Pseudonym (160bits) = Header (8 bits) + Tag Broker Number (12 bits) + Tag Broker Key Id (12 bits) + Modification of Original Tag Value (128 bits) [5].

- Header: Identical with EPC code header. We can use one of reserved value for future use.
- Tag broker Number: For identifying Tag broker Company. Maximum 4096 Tag broker Companies are possible.
- Tag broker Key Id: Used for identifying Tag broker key. Tag broker uses Tag broker key for transformation of 'Original tag value' into 'Tag pseudonym', which would be secure encryption key, such as an AES key.
- Modification of Original Tag Value: Encrypted value of Original Tag Value using Tag Broker Key. Tag Broker must be able to find out Original Tag Value using this value and Tag Broker Key, inversely. We can use AES encryption scheme as transformation method.

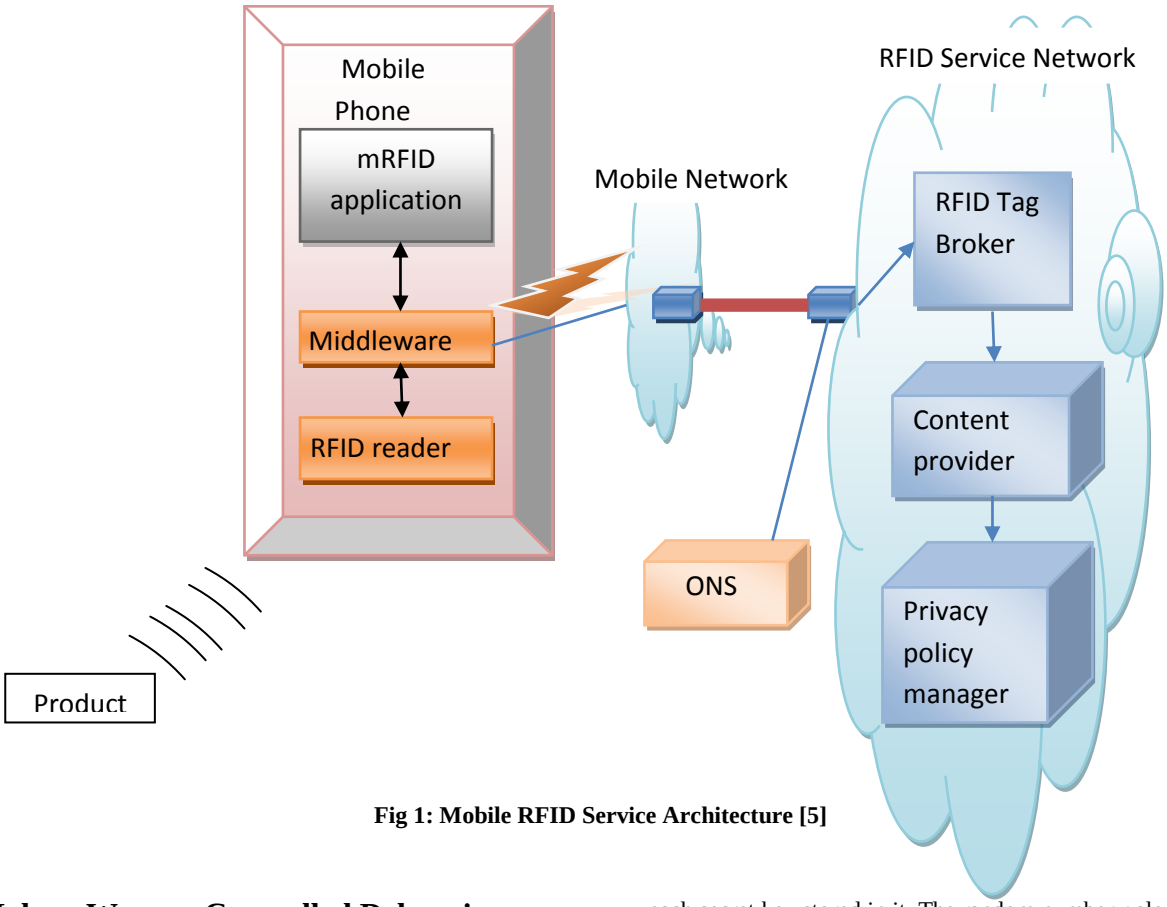

Fig 1: Mobile RFID Service Architecture [5]

2.2 Molnar Wagner Controlled Delegation

The technique suggested by Molnar and Wagner [6, 7] relies on a tree structure to reduce identification complexity. Instead of searching a flat space of secrets, these are arranged in a balanced tree with branching factor. The tags are the leaves of this tree and each edge is associated with a value. Each tag has to store the values along the path from the root of the tree to itself. Upon query, the tag generates a random number r and encrypts it with each secret key stored in it. The random number r along with the cipher texts forms the pseudonym, which is sent to the reader. Reader forwards the same to the Trusted Center (TC), which stores all the secrets, and hence finds mapping between the pseudonym and the tag identifier in O (lg, n) steps. This information is securely returned to the reader after mutual authentication. The Reader has to contact TC for decoding each pseudonym it receives. This communication overhead can be

minimized using the controlled delegation approach suggested in [8].

The concept used here is to allow the reader to perform the mapping itself from a pseudonym (r, p) to the tag's identity ID, but only if the tag's counter value is in a prescribed interval [L, R].

The tree based scheme is an improvement over the earlier hash chain based schemes as it requires only O (lg n) computations, as against O (n) in previous cases. In case of controlled delegation, the search complexity is O (Nr) where O (Nr) is the number of sub trees stored delegated to reader. However, this protocol falls victim to replay attack, as there is only one message from tag to reader. Also, an adversary can tamper with the tag and learn all the secrets stored on it, so there is no forward security. Moreover, these secrets are shared with other tags hence privacy of overall system degrades. A flaw was identified in the paper by Molnar and Wagner [7] on this technique, and correction for the same was proposed, which was acknowledged by the authors [8, 9]. The basic problem earlier was in the secret given to a reader during delegation mechanism. As per the proposed paper, the secret given to the reader enables tag identification beyond the allowed range of the number of times the tags can be read. This is explained by the example below:

Consider the delegation tree shown in Fig 2. To allow reads in interval [2-5], reader is given the secrets S8, S4 and S11, which is the minimal set of nodes that covers the given interval. However, in the original paper, the tag secret at d1 level was given, from which, all the secrets (S1 - S14) can be easily computed.

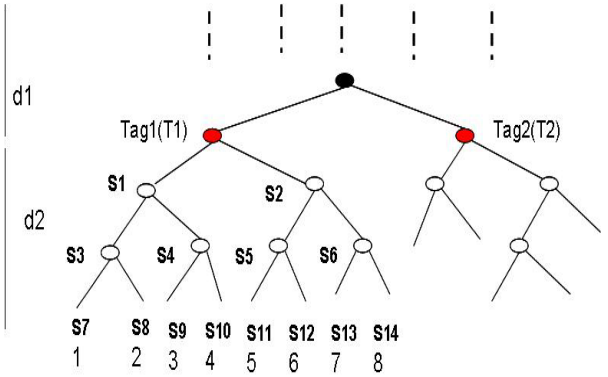

Fig 2: Proposed correction in Molnar Wagner Controlled Delegation Scheme

2.3 The Kill Tag Approach

Kill tag approach is a simple measure for providing privacy and security in RFID systems. In kill tag approach once killed, a tag can never be reactivated. The Auto-ID lab [10] defined a mode of operation for standard supported tags in which a tag could be killed upon purchase of the tagged product. The kill command would require a special 8-bit Password to be sent to the tag. Upon receiving this password the tag would unconditionally erase itself. As "dead tags tell no tales," killing is a highly effective privacy measure. It is envisioned that once RFID tags become prevalent on retail items, point-of-sale devices will kill the RFID tags on purchased items to protect consumer privacy. For example, after you roll your supermarket cart through an automated checkout kiosk and pay the resulting total, all of the associated RFID tags will be killed onthe spot. This would guarantee that no purchased goods contained active RFID tags, satisfying all the security goals and requirements.

Several disadvantages exist with the kill tag approach. The kill command takes a conscience effort to enact; if overlooked it would allow live Tags on items to leave the store. When killing a tag, there is no way to ensure that the kill command was properly executed. With each password being only 8-bits long, a brute force attack using all 256 possible addresses could lead to abuse for malicious purposes. As stated previously, once a tag is killed it can never be re-activated [11].

2.4 Blocking

Blocking scheme depends on the incorporation into tags of a modifiable bit called a privacy bit. A '0' privacy bit marks a tag as subject to unrestricted public scanning; a '1' bit marks a tag as "private". Juels, R.L. Rivest and M. Szydlo (JRS) refer to the space of identifiers with leading '1' bits as a privacy zone [12]. A blocker tag is a special RFID tag that prevents unwanted scanning of tags mapped into the privacy zone. An added advantage to the blocker tag approach is that a blocker tag can be configured to have "Multiple Privacy Zones" allowing ranges of IDs to be blocked while allowing other ranges to operate normally. The selective blocker tag only requires minor changes to a standard RFID tag. A password would be needed to identify privacy zones.

How does a blocker actually prevent undesired scanning? It exploits the anti-collision protocol that RFID readers use to communicate with tags. This protocol is known as singulation. One type of RFID singulation protocol is known as tree walking. A blocker tag, blocks the reader from successfully allowing a tag that is in the interrogation zone to successfully respond with its unique ID number. The blocker tag achieves this by causing a collision for each bit in the request from the reader. In effect this would "jam" tags that the consumer has in their possession, preserving their privacy but allowing the tags to remain active.

2.5 Hash lock

Hah lock, uses the concept of locking and unlocking the tag to allow access. Hash Lock scheme requires implementing cryptographic hash function on the tag and managing keys at the backend. In this scheme, the tag does not reveal its information until the reader sends the right key corresponding to the metaID, which is the hash of the ID [13].

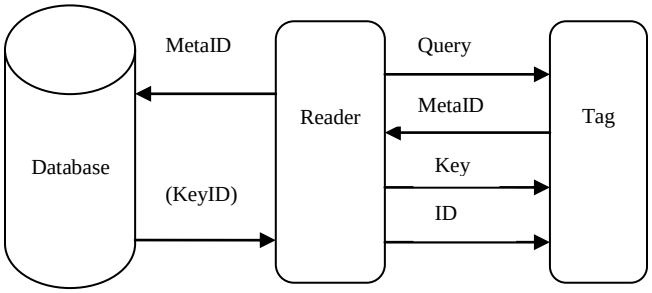

Fig 3: Hash locking reader unlock protocol

Hash Locking: Reader unlocks protocol [13]. To lock the tag the reader sends a hash of a random key, as the meta-ID, to the tag (i.e. meta-ID<- hash (key)). The reader then stores the meta-ID and key in the back end database. While locked, the tag only

responds with the meta-ID when queried. As shown in Fig. 3, to unlock the tag, the reader will query the tag for the meta-ID. The reader will then use the meta-ID to lookup a key and ID for the tag in the database. If the meta-ID is found, the reader then sends the key to the tag in an attempt to unlock the tag. The tag hashes the key and compares the results against the meta-ID stored in the tag. If this compares successfully, the tag will unlock itself and allow access to the reader. It establishes trust between the tags and readers and will prevent unauthorized readers from reading tag contents. By using a meta-ID, tags keep the identity of their holders confidential. The holder has the capability to disable (lock) or enable (unlock) tags, should they desire to do so. Disadvantages include that tags could only be unlocked briefly to minimize the possibility of being hijacked. The use of meta-IDs assumes that the hash function can be implemented in the hardware of low-cost tags with limited resources. The Hash-Lock approach is susceptible to spoofing, using a man-in-the-middle attack for later replay. The meta-ID itself acts as an identifier and may allow tracking of individuals

2.6 Randomized Hash Lock Enhancement

Randomized hash lock proposes an enhancement to the above protocol to help prevent the disclosure of meta-IDs while a tag is in the locked state. Randomizing the tag response during the query process prevents tracking of individuals based on metal ids

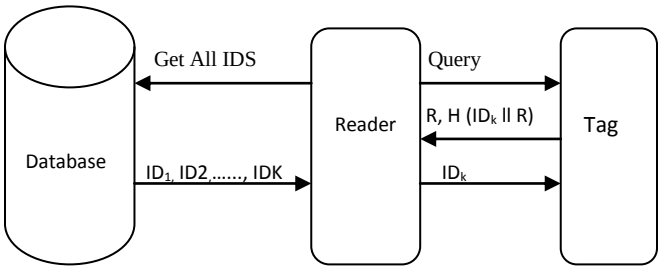

Fig 4 Hash Locking: Enhanced reader unlock protocol using a randomized hash

The randomized Hash-Lock approach requires tags to compute a one-way hash function and include an onboard, random number generator. As shown in Fig 4, a tag responds to a query with a random number r, and a hash of its ID concatenated with random number r. The reader queries the database for all IDs and hashes each ID concatenated with the returned random number r from the tag. If a match is found, the reader sends the ID to the tag for authentication. Disadvantages include a brute force search that must be performed by the reader, making the Hash-Lock randomized approach time consuming and relevant to only a small number of tags. Another disadvantage of the randomized Hash-

Lock protocol is that while a one-way hash function is difficult to reverse, it may still leak bits of its input. Such leaks could compromise the tag's ID value. Moreover, the addition of a random number generator may be costly to implement based on resource constraints.

3. RESULTS AND DISCUSSION

Table 1, shows the strength upto which Molnar Wagner Controlled delegation, Kill Tag, Hash-Lock, Enhanced Hash Lock, Tag Broker Model and Selective Blocker Tag could bear against attacks in RFID (i.e. against some attacks, against all attacks or against only some of attacks).

TABLE 1: Security Requirements in various Protocols

Solution	Meet Security requirements	Reason
Molnar Wagner Controlled delegation	Some	Replay attack is possible, no forward security
Kill tag	All	No active RFId tag
Hash lock	minimum	It is susceptible to spoofing and man in middle attack
Enhanced hash lock	some	It can leak bits of its input which can could compromise the tags ID
Tag broker	all	It uses concept of tag pseudonym which is only known to tag broker and manufacturer
Selective blocker tag	All	A blocker tag prevents unwanted scanning of tags

Table 2, shows the Implementation Cost of Molnar Wagner Controlled delegation, Kill Tag, Hash-Lock, Enhanced Hash Lock, Tag Broker Model and Selective Blocker Tag in RFID (i.e. None, Low, Medium and High).

Table 3, shows the Implementation possibility of Molnar Wagner Controlled delegation, Kill Tag, Hash-Lock Enhanced Hash Lock, Tag Broker Model and Selective Blocker Tag in RFID (i.e. Yes, No or May Be).

TABLE 2: Implementation Cost of various Protocols

Solution	Added cost	Reason
Molnar Wagner Controlled delegation	Medium	We have to maintain a trusted center which stores all the secrets
Kill tag	None	We just give a kill command
Has lock	Medium	We have to maintain a back end data base
Enhanced Hash lock	High	Addition of a random number generator may be costly
Tag broker	Medium	Due to management of tag broker and memory requirement for tag pseudonym
Selective blocker tag	Low	We need to purchase blocker tag

TABLE 3: Implementation Possibility of various Protocols

Solution	Implementation Possibility	reason
Molnar Wagner Controlled delegation	yes	It relies on a tree structure to reduce identification complexity
Kill tag	yes	It uses kill command which can be easily implemented in reader
Hash lock	Yes	It uses concept of metal id which can be easily maintained with the help of back end database
Enhanced hash lock	May be	It uses random number generator which is costly to implement
Tag broker	Yes	Tag broker can be easily merged in mobile RFID service architecture
Selective blocker tag	Yes	Anybody can easily buy a blocker tag

4. CONCLUSION

The discussion of this paper is shown in Table 1, 2 and 3 resulting in selection of different protocol for different usage. Selective Blocker Tag is less vulnerable to security attacks, least practical implementation cost and easy to implement, which is the requirement of practical RFID protocol, which contrast to Enhanced Hash Lock embedded with poor security guard, very costly and hard to implement hence not much usable, for practical implementation.

5. REFERENCES

[1] Damith Ranasinghe, Daniel Engels, and Peter Cole. Low-cost rfid systems: Confronting security and privacy. In Auto-ID Labs Research Workshop, Zurich, Switzerland, September 2004.

[2] Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren, and Kwangjo Kim. Mutual authentication protocol for low-cost RFID. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.

[3] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. Cryptographic approach to privacy-friendly tags. In RFID Privacy Workshop, MIT, MA, USA, November 2003.

[4] G. Avoine, P.Oechslin, "RFID Tracebility: A Multilayer Problem". In Financial Cryptography, 2005.

[5] Sokjooon Lee, Howon Kim and Kyoil Chung, "Tag Broker Model for Protecting Privacy in RFID Environment". World Academy of Science, Engineering and Technology 10, 2005.

[6] Gildas Avoine. Cryptography in Radio Frequency Identi_cation and Fair Exchange Protocols. PhD thesis, EPFL, Lausanne, Switzerland, December 2005.

[7] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In Marc Joye and Jean-Jacques Quisquater, editors, Workshop on Cryptographic Hardware and Embedded Systems - CHES 2004, volume3156 of Lecture Notes in Computer Science, pages 357-370, Boston, Massachusetts, USA, August 2004. IACR, Springer-Verlag.

[8] David Molnar, Andrea Soppera, and David Wagner. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In Bart Preneel and Sta_ord Tavares, editors, Selected Areas in Cryptography - SAC 2005, Lecture Notes in Computer Science, Kingston, Canada, August 2005. Springer-Verlag.

[9] Gildas Avoine and Philippe Oechslin. A scalable and provably secure hash based RFID protocol. In International Workshop on Pervasive Computing and Communication Security - PerSec 2005, pages 110{114, Kauai Island, Hawaii, USA, March 2005. IEEE, IEEE Computer Society Press.

[10] MIT Auto-ID Center. http://www.autoidcenter.org, Feb 2004.

[11] Ari Juels. RFID security and privacy: A research survey. Manuscript, September 2005.

[12] A. Juels, R.L. Rivest, M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In v Atluri, editor 8th ACM Conference on Computer and Communications Security, paaes 103-111. ACM Press, 2003.

[13] S.A.Weis, S.E.Sarma, R.L. Revest, D.W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems" accepted for publication to the First International Conference on Security in Pervasive Computing (SPC 2003),March 12-14,2003.