Volume-4, Issue- 1
Jul – Dec, 2018

ISSN : 2581 - 4125

HMR Interdisciplinary Journal of Science, Technology & Education Management

HMR Institute of Technology & Management
(Affiliated to Guru Gobind Singh Indraprastha University, Delhi)
Hamidpur, Delhi – 110 036

HMR INTERDISCIPLINARY JOURNAL OF SCIENCE, TECHNOLOGY AND EDUCATION MANAGEMENT

Advisory Board

Editorial Board

ABOUT THE JOURNAL – HMRIJSTEM

(ISSN: 2581-4125)

HMR Interdisciplinary Journal of Science, Technology & Education Management is published by HMR Institute of Technology & Management, Hamidpur, Delhi, on bi – annual basis with the aim to provide a suitable platform presenting well considered, meaningful, constructively thought provoking, non-political and non controversial but critically analyzing and synthesizing present and future aspects of technical and interdisciplinary education particularly reference to our country. The authors and contributors are expected to highlight various research issues along with meaningful suggestions for solution, refinement and innovations.

Authors are requested to follow the IEEE Conference Paper Template. The authors are fully responsible for the contributions. Articles will be selected by the Editorial Board and are subject to editorial modification, if necessary. All data, views opinion etc being published are the sole responsibility of the author. Neither the publisher nor the HMRITM is anyway responsible.

THERE IS NO PUBLICATION FEE.

For detail regarding guidelines, copyright and paper template visit Institute website: www.hmritm.ac.in

Paper / Manuscripts are invited for Jan – June Issue and Jul – Dec Issue

Send your manuscripts to editor.journal@hmritm.ac.in

Editorial

We, at HMRITM are delighted to announce the release of Volume 4, Issue 1, of HMR Interdisciplinary Journal of Science, Technology and Education Management. HMRIJSTEM publishes articles which present novel research in the areas of engineering, science, technology and management. The Editorial Team encourages interdisciplinary research and the current issue publishes seven research papers and the efforts of all the corresponding author' s are significant for the successful operation of the journal.

This edition of HMRIJSTEM contains articles "RFID in Anti-Cloning and Security", "Cryptography using Neural Network", "Data Integrity and Authentication in WSNs", "Water Quality Analysis using Arduino" and "Yojana Access: All schemes on one click".

We take this opportunity to thank all those contributors, reviewers, in making this issue an unforgettable one. We would also like to thank our Chief Patron - Hon'ble Shri A K Gupta, Our mentor Prof Ramjee Prasad, Founder Chairman, Global ICT Standardization Forum for India (GISFI), AARHUS University, Herning Denmark, Chief Executive Officer - Mr S N Jha (IAS – Retired) , Director - Prof V C Pandey, Deputy Director - Prof Shalini Gupta and all Advisory Board Members for their motivation and support in bringing out this edition of HMRIJSTEM. Suggestions and feedback from our readers are welcome for the overall improvement of quality.

Delhi
15/01/2019

Editorial Board

RFID in Anti-Cloning and Security

Faheem Ahmad

Shri Venkateshwara University, Gajraula, Uttar Pradesh, India
fah.ahmad@gmail.com

Abstract— RFID systems are emerging as one of the most pervasive computing technologies. But there are still a large number of problems that are to be addressed. One of the fundamental issues still to be addressed is privacy, which concludes association threat, location threat, preference threat, constellation threat, transaction threat, action threat and breadcrumb threat (Kim, J., Yang, C, Jeon, J,2007). Misbehaviours of both readers and tags will lead to attacks to the system. The common attacks on the readers, tags and the air interface between them comprise: Tracking or Tracing, Tamper, Clandestine scanning, Counterfeit tags, Cloning tags, Eavesdropping, Replay, man-in-the-middle attack, Spoofing, Differential power analysis, Timing Attacks, Denial of Service, Physical Attacking and so on. A number of mechanisms have been devised to overcome the problems related to security and privacy issue of RFID systems. In this paper we propose three anonymous RFID authentication protocols and prove that they are secure in the traditional cryptographic framework. Our model allows most of the threats that apply to RFIDs systems including, denial of service, impersonation, malicious traceability, information leakage through power analysis and active man-in-the middle attacks. Our protocols are efficient and scalable.

Keywords— RFID; Authentication; Privacy; Scalability; Counterfeiting; Cloning.

I. INTRODUCTION

RFID (Radio-Frequency IDentification) is a technology for automated identification of objects and people. Human beings are skillful at identifying objects under a variety of challenge circumstances. RFID may be viewed as a means of explicitly labelling objects to facilitate their "perception" by computing devices. An RFID device – frequently just called an RFID tag – is a small microchip designed for wireless data transmission. It is generally attached to an antenna in a package that resembles an ordinary adhesive sticker. The microchip itself can be as small as a grain of sand, some 0.4mm2 [1]. An RFID tag transmits data over the air in response to interrogation by an RFID reader. Today, large organizations, such as Wal-Mart, Procter and Gamble, and the United States Department of Defense are deploying RFID as a tool for automated oversight of their supply chains. Thanks to a combination of dropping tag costs and vigorous RFID standardization, we are on the brink of an explosion in RFID use.

RFID is supposed to be the successor of the optical barcode printed on consumer products, with two individual advantages:

- Unique identification: A barcode indicates the type of object on which it is printed, e.g., "This is a 50 grams bar of XYZ brand 70% chocolate." An RFID tag goes a step ahead. It emits a unique serial number that distinguishes among many millions of identically manufactured objects; it might indicate, e.g., that "This is 50 grams bar of XYZ brand 70% chocolate, serial no. 887891873." The unique identifiers in RFID tags can act as pointers to a database entries containing rich transaction histories for individual items.
- Automation: Barcodes, being optically scanned, require line-of-sight contact with readers, and thus watchful physical positioning of scanned objects. Except in the most rigorously controlled environments, barcode scanning requires human intervention. In contrast, RFID tags are readable without line-of-sight contact and without precise positioning. RFID readers can scan tags at rates of hundreds per second. For example, an RFID reader by a warehouse dock door can today scan stacks of passing crates with high accuracy. In the future, point-of-sale terminals may be able to scan all of the items in passing shopping carts [2].

The main form of barcode-type RFID device is known as an EPC (Electronic Product Code) tag. An organization known as EPCglobal Inc. [3] oversees the development of the standards for these tags. Not surprisingly, EPCglobal is a joint venture of the UCC and EAN, the bodies that regulate barcode use in the United States and the rest of the world respectively. EPC tags cost and RFID readers cost are dropping drastically [4].

In general, small and inexpensive RFID tags are *passive*. They have no on-board power source; they derive their transmission power from the signal of an interrogating reader. Passive tags can operate in any of a number of different frequency bands. LF (Low-Frequency) tags, which operate in the 124 kHz – 135 kHz range, have nominal read ranges of up to half a meter. HF (High-Frequency) tags, operating at 13.56 MHz, have ranges up to a meter or more (but typically on the order of tens of centimetres). UHF tags (Ultra High-Frequency), which operate at frequencies of 860 MHz – 960 MHz (and sometimes 2.45GHz), have the longest range – up to tens of meters. UHF tags, though, are subject to more ambient interference than lower-frequency types. In this paper, we enumerate the major standards for passive RFID devices. Some RFID tags contain batteries. There are two such types: *semi-passive* tags, whose batteries power their circuitry

when they are interrogated, and *active* tags, whose batteries power their transmissions. Active tags can initiate communication, and have read ranges of 100m or more. Naturally, they are bit expensive.

II. RFID TODAY AND TOMORROW

Many of us already use RFID tags routinely. Examples include:

- Proximity cards, that is, the contactless cards used for building access.
- Automated toll-payment transponders – the small plaques mounted in automobile windshields. (These are usually semi-passive).
- The ignition keys of many millions of automobiles, which include RFID tags as a theft-deterrent.
- Payment tokens: In the United States, the SpeedPass™ token for petrol station payments is an example. Contact-less credit-cards, like American Express ExpressPay™ and the Mastercard PayPass™ use RFID.

Millions of house pets around the world have RFID tags implanted in their bodies, to facilitate return to their owners should they become lost.In the world of the future – amazing things would be possible. Here are a few possibilities that the reader might dream up:

- **Smart appliances:** By exploiting RFID tags in garments and packages of food, home appliances could operate more cleverly. Washing machines might select wash cycles automatically, for instance, to avoid damage to delicate fabrics. Your refrigerator might warn you when the milk has expired or you have only one remaining carton of yogurt – and could even transmit a shopping list automatically to a home delivery service [5].
- **Shopping:** In retail shops, consumers could check out by rolling shopping carts past point-of-sale terminals. These terminals would automatically tally the items, compute the total cost, and perhaps even charge the consumers' RFID-enabled payment devices and transmit receipts to their mobile phones. Consumers could return items without receipts. RFID tags would act as indices into database payment records, and help retailers track the pedigrees of defective or contaminated items.
- **Interactive objects:** Consumers could interact with RFID-tagged objects through their mobile phones. (Some mobile phones already have RFID readers.) A consumer could scan a movie poster to display show times on her phone. She could obtain manufacturer information on a piece of furniture she likes by waving her phone over it.
- **Medication compliance:** Research at Intel and the University of Washington [6] exploits RFID to facilitate medication compliance and home navigation for the elderly and cognitively impaired. As researchers have demonstrated, for example, an RFID-enabled medicine cabinet could help verify that medications are taken in a timely fashion. More generally, RFID promises to bring tremendous benefits to hospitals [7].

But what, really, is "RFID"?

We have discussed the basics of RFID and laid out some evocative scenarios. Yet we have not formally defined the term "RFID." A wholly satisfying definition is elusive. ut it is not a mere pedantic exercise: The definition of RFID can have an important impact on technical and policy discussion [8]. In this paper, we use "RFID" to denote any RF device whose main function is identification of an object or person. At the rudimentary end of the functional spectrum, this definition excludes simple devices like retail inventory tags, which merely indicate their presence and on/off status. It also excludes portable devices like mobile phones, which do more than merely identify themselves or their bearers. A broad definition for "RFID" is appropriate because the technical capabilities and distinctions among RF devices will drift over time, and the privacy and authentication concerns that we highlight in this paper apply broadly to RF identification devices great and small. Most importantly, though, the names of standards like 'ISO 14443" or "EPC Class-1 Gen-2" do not trip off the tongue or inhere well in the mind.

III. CONCEPTUAL MODELS

An RFID authentication system has three components: tags T, readers R, and a trusted server S. Tags are wireless transponders: they typical have no power of their own and respond only when they are in an electromagnetic field. Readers are transceivers and generate such field: they challenge by broadcast any responding tag. There are two types of broadcast challenges: multicast and unicast. Multicast challenges are addressed to all tags in the range of the reader, whereas unicast challenges are addressed to specific tags. In our protocols below we have both types of challenges. However, our multicast challenges are just random strings, and all tags in the range of a reader R are challenged with the same random string. This kind of action is not usually counted as a communication pass.

We shall assume that all "honest" tags T adhere to the system specifications and the requirements of the authentication protocol. The same applies for the readers R and of course the trusted server S - they are all "honest". Tags are issued with private keys K which they share (only) with the trusted server S. These keys are used by the tags for identification. We denote by K the set of all authorised keys (issued by S). Figure 1 illustrates the flow of exchanged data between a tag T and the trusted server S via the reader R, during the authentication of T.

$$T \leftrightarrow R \Leftrightarrow S$$

Fig. 1. The authentication flow in an RFID system

We shall refer to the interaction between T and R as a conversation and the data as an authentication transcript. In our RFID authentication protocols we shall assume that R and S are linked by a secure communication channel (reliable and authenticated). Therefore, our protocols are essentially two party protocols, one party being a tag T and the other a reader $R = R^S$, with secure access to a server S. These parties are abstracted as probabilistic Turing machines. T-machines with severely restrained resources, and R-machines with adequate resources. For "optimistic" authentication protocols, the resource must be minimized for both machines.

This model describes the setting for the "honest" parties: the tags that are authenticated with private keys $K \in \mathcal{K}$, that adhere to the protocol, the readers R that adhere to the protocol, and the trusted server.

IV. Attacks on RFID

When designing secure RFID authentication protocols one should also take into account attacks that are excluded from the security model used (the system). Sometimes these attacks may be prevented by using out-of-system protection mechanisms. Of course, it is preferable to deal with such attacks within the model. Below we list two such attacks:

A. The Adversary

The adversary A can control a certain number of tags and readers. The tags of the adversary, denoted by T´ are unauthorised, in the sense they do not have a private key $K \in \mathcal{K}$. Similarly, the readers of the adversary, denoted by R´, are unauthorized, in the sense that they do not have authenticated access to the trusted server S.

An active adversary A can modify the conversations between any pair T, R arbitrarily (e.g. adaptively and concurrently), and indeed initiate and terminate a session, at its choice. As an extension of a passive (eavesdropping) adversary, A is also allowed to learn the output of the session, i.e. the reader's decision to accept or not, at the end of every sessions. Since the channel between a reader R and the server S is assumed secure (authenticated), we do not need allow A to interact with the server S directly, but only through (honest) readers. When designing secure RFID authentication protocols one should also take into account attacks that are excluded from the security model used (the system). Sometimes these attacks may be prevented by using out-of-system protection mechanisms. Of course, it is preferable to deal with such attacks within the model.

B. Types of Attacks

When designing secure RFID authentication protocols one should also take into account attacks that are excluded from the security model used (the system). Sometimes these attacks may be prevented by using out-of-system protection mechanisms. Of course, it is preferable to deal with such attacks within the model. Below we list such attacks:

C. Side Channel Attacks (Power Analysis Attacks)

These are attacks in which the private key of a device is extracted by exploiting either its power consumption when inaccurate/accurate received bits are processed or the variations in the timing of its energy output. This is the idea of simple and differential power analysis was first introduced by Kocher [9]. This is a serious threat. Thus implementers need algorithms that are not only efficient but also SCA registrant.

D. Online Man-in-the-Middle Relay Attacks

These are attacks in which an unauthorised reader R´ and tag T‘ interpose between an authentic tag T and reader R so that, the authentication flow in (T, R, S) is diverted to a flow (T, R´, T´, R, TS) that authenticates the imposter T‘ using the authentication data of T.

E. Online Man-in-the-Middle Active Attacks

These are attacks in which an unauthorized reader R´ and tag T´ interpose between an authentic tag T and reader R so that, when R´ challenges T appropriately in (T, R´), the data obtained will leak private information of T when input to (T´R, S).

V. Security in RFID

The security of an RFID protocol can be described in terms of three games, an authentication game G_{auth}, an anonymity game G_{anon}, G_{anon}, a tracing game G_{trace} and an availability game G_{avail}, with players: the adversary A against the honest tags T and the honest readers R. In these games there are two steps. The first step is a preparing step for the adversary A: A is allowed to interact arbitrarily with the tags and the readers. In the second step, A's knowledge is tested. The score of A in game G is his advantage adv A G. A wins if his advantage is non-negligible. We now describe in more detail the second steps of the four games: G_{auth}, G_{trace}, G_{anon} and G_{avail}.

A. Authentication

The authentications are done in two ways. By authenticating a reader to a tag, a tag is to be ready to open its information to a reader, and by authenticating a tag to a reader, the system prohibits the usage of fake tags. We can divide published authentication protocols into two types. The first type is the fixed access control in which a tag replies a reader with a fixed message. The second type is the randomized access control in which a tag replies to a reader with a pseudo-random message which varies each time of the responses. The fixed access control is the simplest type so that tags can be implemented in a cheap price. However, this kind of protocols is under the tracking problem [10], proposed a fixed access control using a hash based access control, where tags reply with MetaIDs, which are the hash outputs of their real IDs. Even though attackers cannot figure out the real ID,

the constant responses of tags cause the tracking problem. A solution to prevent the tracking problem is the randomized access control. In order to randomize messages, a reader and a tag need to share some secret information which is unknown to attackers so that only the entities which have the secret information can interpret the randomized messages. Again, the randomized access control can be divided into two types depending on whether all the readers and the tags share the same secret information. Without sharing the common secret information among all the readers and the tags, making the response pseudo-random causes some drawbacks. [10] described protocols which resolve tracking problems, but the systems are not scalable since the server needs to perform hashes for all the tags ID every time of authentication protocols. One approach to resolve the un-scalability of randomized access control is proposed in [11]. This scheme used a cryptanalytic method. However, this method also causes some other problems. Since this protocol uses time-memory trade-off method [11], in order to reduce the searching time they have to increase the amount of memory in the server. Another problem is that the searching algorithm is probabilistic, i.e. there is some probability to fail in searching for a tags ID. Even though they are saying the failure probability is small, it can cause a crucial problem in certain applications. Protocols proposed in [12] [13] resolve the tracking problem by sharing the common secret information among all the readers and the tags. Even though these schemes are scalable and resolve the tracking problem, they have a crucial problem. By capturing and compromising only one tag, attackers can reveal the secret information. Once the secret information is revealed, the tags which share the secret information will be under attack and attackers may clone some other tags. Moreover, the protocol in [14] uses a symmetric key encryption algorithm which is unsuitable in low-cost RFID systems.

In the second step of G_{auth}, A must impersonate some tag T to some reader R. During this impersonation step, A is allowed to interact arbitrarily with all other tags and readers, except the one tag T that A is trying to impersonate.

The advantage of the adversary adv A G_{auth} is the probability that A succeeds in authenticating itself to R. An RFID protocol is a secure authentication protocol if adv A G_{auth} is negligible. We have excluded A from interacting with the tag T from the second step because this seems to correspond to reality: if A were allowed to interact with T as a reader R during this step, and then simply relay faithfully the conversation between T and R‘ to an authorised reader R in order to get authenticated as T (without mounting any attack). This is the online man-in-the middle attack described above in Untraceability is a weak notion of anonymity. In the second step of the tracing game G_{trace}, A must trace some tag T: A is given access to (i.e. ability to interact with) a challenge tag T* and must tell whether T*, is T or not, better than guessing. In this tracing step, A is also allowed to interact with all tags and readers, in particular, interacting with T. This is the advantage adv A G_{trace} of the adversary in this game.

B. *Untraceability*

Untraceability is a weak notion of anonymity. In the second step of the tracing game G_{trace}, A must trace some tag T: A is given access to (i.e. ability to interact with) a challenge tag T* and must tell whether T*, is T or not, better than guessing. In this tracing step, A is also allowed to interact with all tags and readers, in particular, interacting with T.

The advantage adv A G_{auth} of the adversary in this game is $|\text{Prob}[\text{A correct}] - ½\ |$,

where $\text{Prob}[\text{A correct}] = \text{Prob}[\text{A} = \text{yes}|\text{T} = \text{T‘}] + \text{Prob}[\text{A} = \text{no}|\text{T} \neq \text{T‘}]$ and we require that $\text{Prob}[\text{T} = \text{T‘}] = ½$.

We have untraceability if advA G_{trace} is negligible.

C. *Unlinkability*

Unlinkability is a strong notion of anonymity, which is the one we use in this paper. For anonymity we require that the advantage adv A G_{anon} of the adversary in the second step of G_{anon} in linking two different interactions to the same tag is negligible. The setting for G_{anon} is the same as in G_{trace}, except that in G_{trace} the adversary already knows T through other interactions in the first step. In G_{anon} both T and T* are challenge tags. Through interacting with T and T* ,as well as all other normal tags and readers, A must tell whether it is interacting with identical tags or not, i.e. whether T and T* have the same key $K \in \mathcal{K}$ or not.

D. *Availability*

In G_{avail} the adversary A must prevent a tag T from being authenticated by a reader R in a challenge session ses, without interacting with this session ses. In this attack, A is allowed to interact with all tags and all readers, except of course for the session ses. The advantage adv A G_{anon} of A in this game is the probability that R rejects T in the challenge session ses. For completeness of an authentication protocol P, we explicitly require that: for all authorized tags T and readers R, P accepts with overwhelming probability. We note that this is implied implicitly in the availability game G_{avail}.

VI. RFID Models To Deal with Counterfeiting and Attacks

In order to protect a product against cloning (counterfeiting) a detection mark is embedded into the product or its packaging. This detection mark consists of a physical and a digital part. The mark is put there by a legitimate authority. The attacker (counterfeiter) has access to all components of this detection mark; i.e. she can read it, remove it from the product and investigate it. Based on the information that she obtained from investigating the legal detection mark, she produces a fake detection mark. The goal of the attacker is to produce a fake detection mark that can

only with small probability be distinguished from an authentic one.

A. Components of Anti-Counterfeiting Technology

In order to protect a product against counterfeiting, technological means are needed to verify whether the product is authentic or not. In order to make an item unclonable, the following two components are needed.

Physical protection. This is obtained by using unclonable physical structures embedded in the package (removal of the structure leads to its destruction). One or more unique fingerprints derived from the physical structure will be printed on the product for the verification of the authenticity of the product.

Cryptographic protection is serving two goals. Firstly, cryptography provides techniques (digital signatures) to detect and prevent tampering with data (fingerprints) derived from a physical object. Secondly, it provides secure identification protocols to identify a product. Those protocols do not leak any necessary identification information to an eavesdropper attacking (actively or passively) the communication channel.

Good candidates for uncolnable physical structures that can be used for physical protection purposes, are so-called Physical Unclonable Functions (PUFs) [15].

B. General Anti-Counterfeiting Protocol

We give intuition for protocols that can be used to check the authenticity of a product based on embedding a PUF in the product in combination with the use of cryptographic techniques.

First there is an enrollment phase, which is performed by some trusted authority. During this phase the following steps are performed.

- Several fingerprints are derived from the PUF by challenging it with multiple challenges and recording the responses. These responses are then turned into binary fingerprints (and some auxiliary data are derived for use during the verification phase).
- These challenges, fingerprints and auxiliary data are then signed with the secret key *sk* of the issuer of the product (the issuer is assumed to be trustworthy).
- The signatures, the challenges (corresponding to the fingerprints) and may be some auxiliary data (needed to perform processing during the authentication phase) are also printed on the product (and/or stored in a database).

During the verification phase, the authenticity is checked by running the following protocol.

- The verification device reads the challenges and auxiliary data.
- The verification device challenges the physical structure with one of the challenges printed on the product. After having measured the responses, it derives the fingerprint from the response based on the auxiliary data.
- Then, using the fingerprint derived in step 2, the verification device checks the signature to verify that the fingerprint, challenges and auxiliary data were printed on the product by a legitimate authority. If the signature is not correct, the product is not authentic.

We briefly analyze the security of this protocol. An attacker who wants to counterfeit the product has to embed a fake physical structure on the product that produces correct fingerprints to the challenges (with correct signatures). Under the assumption that the physical structure is unclonable, she cannot produce a clone of the originally embedded physical structure. More precisely, we assume that given some challenges c_1 …., c_n and corresponding fingerprints s_1….,s_n she cannot produce a (fake) physical structure that produces the same fingerprints s_1…., s_n given the original challenges c_1…., c_n. On the other hand she can produce another structure and create challenges, auxiliary data and fingerprints s'_1…., s'_n according to the procedures used during enrollment. However, since she does not know the secret key *sk* and the responses of her fake structure will be different with very high probability, she will not be able to put the correct signatures on these data. The verification device will detect that the signatures are not correct and reject this as a fake product. We note that the number of fingerprints that can be verified during a verification session is very limited by time and space constraints. Furthermore, the attacker can easily capture the required fingerprints (by measuring the responses according to the challenges printed on the product). Therefore the production of a clone only requires the fabrication of a physical structure (PUF) producing the same fingerprints for a limited number of challenges.

The PUF based solution for preventing counterfeiting of goods that was presented above can be improved with active components, that are inseparably linked with a PUF. An example consists of an RFID-tag equipped with a microchip that is inseparably bound to a PUF. Because of the presence of a microchip a secure identification protocol can be run without revealing any information on the fingerprint of the PUF. Additionally, by inseparably linking the chip and the PUF, it becomes possible to prevent leakage of the PUF measurement to the outside world.

Typical RFID systems consist of the following two components: the *RFID-tag* and a *reader*. The reader will perform the verification to detect whether a tag is authentic or not. The RFID-tag consists of an antenna connected to a microchip that can store and read data and has possibly some

dedicated hardware to perform a small amount of computations. Typically, the power for performing operations is obtained from the RF-field (by inductive coupling). A reader can read and write data from/on a tag. The reader is often linked with some system that can perform computations on the data that it receives from tags.

In order to use RFID-tags for anti-counterfeiting purposes, we proceed as follows. An RFID-tag containing reference information is embedded in a product. The (identification) data stored in the memory of the tag is signed with the secret key *sk* of the legitimate issuer. The tag communicates with a reader for verification purposes over a public channel. The ROM memory of the tag is accessible to the attacker. The reader has a certified public key *pk* corresponding the issuer's secret key for verification of the digital signatures.

C. Power Analysis Attacks

Our RFID authentication protocols in the next section are designed to deal with power analysis attacks and offline man-in-the middle active attacks. For the online man-in-the middle attacks an \out-of-system" solution should be sought.

In this section we propose three RFID authentication protocols, a 2-pass authentication protocol and two 1-pass authentication protocols. The last protocol is optimistic, in the sense that its cost is low when the adversary is passive. We shall prove that these are secure using our security model, and that the tags are untraceable. These protocols address most of the drawbacks of the authentication protocols in [16, 17, 19, 18, 20], and will also thwart power analysis attacks. Our first protocol is an extension of YA-TRAP proposed by G. Tsudik [19] which we briefly describe below.

- YA-TRAP [Yet Another Trivial Authentication Protocol]For this protocol, the timeline is divided into small periods, during which each tag is allowed to be authenticated at most once. The readers and the server maintain a (loosely) synchronized timestamp tsys. The tags do not have clocks. Each tag T is equipped with a pseudo-random number generator (which may be resolved as an iterated keyed hash function), and is initialized with a private key K and timestamps t0 and tmax, K is the set of all keys that have been issued to tags.When a reader R activates tag T, it broadcasts the current timestamp t_{sys}. If $t_{sys} <= t_{tag}$, where t_{tag} was the last timestamp that T received, or if $t_{sys} > t_{max}$, then T broadcasts a pseudorandom string; otherwise T broadcasts $h = H_K(t_{sys})$, and sets $t_{tag} = t_{sys}$. Here $H_K(t_{sys})$ is the hash of t_{sys} with key K, and t_{tag} is initialized with the value t_0.

  The server S finds the value of the key that T has used in h from a hash look-up table - see Figure 2. In this table, whenever a timestamp t_s is updated, the server computes the keyd hash values $H_K(t_s)$ for all keys $K \in \mathcal{K}$, and get the next row of the table. This table, $\{h_{i,j} = H_{Ki}(j)\}$, makes it possible for the server S to find out whether the tag T that issued the hash h is authentic, $h = h_{tsys;j}$ for some $j \in [1, n]$, without having to search exhaustively for the key each time a new tag is challenged during time period t_s (typically one or a few minutes).

	K_1	K_2	$\cdots$	K_n
$t_s = 1$	$h_{1,1}$	$h_{1,2}$	$\cdots$	$h_{1,n}$
$t_s = 2$	$h_{2,1}$	$h_{2,2}$	$\cdots$	$h_{2,n}$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
$t_s = i$	$h_{i,1}$	$h_{i,2}$	$\cdots$	$h_{i,n}$

Fig. 2. The hash look-up table.

Tsudik points out [19] that there is a drawback in YA-TRAP: the adversary can send a wildly inaccurate timestamp t'_{sys} (say the maximum timestamp allowed) and incapacitate the tag. This is a DoS attack which will kill the tag. It quite is difficult to address this attack since the tag T needs to update its time t_{tag} regardless of the value of the time t'_{sys} sent by adversary, otherwise its identity will be traced by sending the same t'_{sys} every time. To avoid tracing, it is not sufficient to randomize the tag's response since that would eliminate the savings that the server gets from using the look-up table.

There is also a “future-time” attack in which the adversary queries the tag offline with several valid time periods $t_{sys;i}$, i = 1, 2 , , , . .. The adversary then captures the tag's responses and can use that for online authentication when these time periods. Therefore, by using a predictable time value as a challenge for the tag will not work. In the following section we show who to deal with these attacks while keeping the server scalable by adapting the protocol YA-TRAP.

- A 2-Pass Optimistic Anonymous RFID Authentication Protocol
  YA-TRAP is (essentially) a 1-pass protocol, in the sense that the timestamp is broadcast (not unicast) by R to all tags in range. We now show that how to extend YA-TRAP to deal with the DoS attack in which the adversary disables the tag T by sending an inaccurate timestamp.

The protocol we propose is essentially a 1-pass authentication protocol with an optional pass. In the first step the tag is authenticated, whereas in the second step the server authenticates the timestamp. The protocol is given in Figure 3.

R broadcasts (t_{sys}, r_{sys}).

1. $T \to R \to S$: $r_{tag},\ h_1 = H_K(0, t_{sys}, r_{sys})$ if $t_{sys} > t_{tag}$
   $r_{tag},\ h_1 = H_K(1, r_{tag}, r_{sys})$ if $t_{sys} \le t_{tag}$
2. $S \to R \to T$: $r_{tag},\ h_2 = H_K(2, r_{tag}, t_{sys})$ (optional)

– S accepts T as authentic only if:
$\exists K \in \mathcal{K} : (h_1 = H_K(0, t_{sys}, r_{sys})) \vee (h_1 = H_K(1, r_{tag}, r_{sys}))$.
– T verifies that $h_2 = H_K(2, r_{tag}, t_{sys})$. (optional)
– T sets $t_{tag} = t_{sys}$ if $t_{sys} > t_{tag}$.

Fig. 3. A 2-Pass optimistic anonymous RFID authentication protocol

In our protocol the tag T, instead of sending a pseudo-random string when the timestamp it gets is out of its bounds, it sends a keyd hash of the string (1, T_{tag} , t_{sys}). This will save the tag T, but now the server S must work harder. More specifically, if the hash value h is not in the look-up table (see Figure 2), then the server must search exhaustively for the key K. Of course, this only happens with tags that the adversary has tried to kill (or incapacitate).

Our approach is to shift the adversary's attack from the low complexity tags to the server. This approach is optimistic, in the sense that when the adversary is passive than the server need only use the look-up table. Note that pass 2 is optional. This pass is only used by the server during time periods when a number of attacks occur beyond a certain threshold and the server would like to resynchronize the time t_{sys} to all the tags so that their stored time t_{tag} is valid.

This is applied to all tags during such time periods so that no identity information are revealed. When this period passes, the server could return to normal operation and will bypass pass 2. This makes the scheme resistant to DoS while being almost as efficient as [19].

- A 1-Pass Optimistic Anonymous RFID Authentication protocol

$keys$	K_1	K_2	$\cdots$	K_n
$strings$	r_{K_1}	r_{K_2}	$\cdots$	r_{K_n}

Fig. 4. A look-up string table.

This protocol uses a key lookup table in which the keys K are linked to session number T_K, see Figure 4. The optimistic protocol is described in Figure 5 and is only one pass.

R broadcasts r_{sys}.

1. $T \to R \to S$: $r_{tag},\ h = H_K(r_{sys}, r_{tag})$

– T updates $r_{tag} \leftarrow H_K(r_{tag})$.
– S accepts T only if:
$\exists K$: (r_{tag}, K) are in the key look-up table s.t.: $h = H_K(r_{sys}, r_{tag})$ (optimistic)
OR $\exists K \in \mathcal{K}$ such that $h = H_K(r_{sys}, r_{tag})$ (exhaustive search)
– S updates $r_{tag} \leftarrow H_K(r_{tag})$.

Fig. 5. A 1-Pass anonymous RFID authentication protocol

The protocol described in Figure 5 always uses only one pass. When a tag has been attacked, its pseudo random value T_{tag} will be out-of-sync with its counterpart s_K stored in the server. At this time, the server will have to search for all keys to find the correct one and then resynchronize s_K. Even when this happens, the scheme has the advantage that the server only needs to do extra computation for tags that are authenticated, not for all the tags. When no fault occurs, the server simply has to do one lookup and hashing for each authenticating tag. So computation is saved on tags that do not communicate.

In the non-optimistic version of this protocol, the tag and server uses true random T_{tag} and therefore the server needs to search and udpate its value for any tag that requires authentication. This scheme is suitable for cases where the number of active tags is smaller than the number of tags.

VII. Conclusion

It is astonishing how a modest device like an RFID tag, essentially just a wireless license plate, can give rise to the complex melange of security and privacy problems that we explore here. RFID privacy and security are stimulating research areas that involve rich interplay among many disciplines, like signal processing, hardware design, supply-chain logistics, privacy rights and cryptography.

An important aspect of RFID security is that of user *perception* of security and privacy in RFID systems. As users cannot see RF emissions, they form their impressions based on physical cues and industry explanations. RFID will come to secure ever more varied forms of physical access and logical access. To engineer usable RFID systems and permit informed policy decisions, it is important to understand how RFID and people mix.

Both the physical cloning attack as well as the cloning attack based on (actively or passively) attacking the protocol between the tag and the reader can be prevented. It has been

shown that the required protocols are feasible on an RFID-tag in the offline situation.

REFERENCES

[1] C.F. Hernández, P.H. Ibargüengoytia-González, J.G. Hernández, J.A. Díaz, "Wireless Sensor Networks and Applications: a Survey", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, Pages 264 -273. March 2007.

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

[2] D. White. NCR: RFID in retail. In S. Garfinkel and B. Rosenberg, editors, RFID: Applications, Security, and Privacy, pages 381–395. Addison-Wesley, 2005.

[3] EPCglobal Web site, 2005. Referenced 2005 at http://www.EPCglobalinc.org.

[4] S. E. Sarma, S. A. Weis, and D.W. Engels. RFID systems, security and privacy implications. Technical Report MIT-AUTOID-WH-014, AutoID Center, MIT, 2002.

[5] Merloni unveils RFID appliances. RFID Journal, 4 April 2003. Referenced 2005 at http://www.rfidjournal.com/article/articleview/369/1/1/.

[6] K. P. Fishkin, M. Wang, and G. Borriello. A ubiquitous system for medication monitoring. In Pervasive 2004, 2004. Available as 'A Flexible, Low-Overhead Ubiquitous System for Medication Monitoring, Intel Research Seattle Technical Memo IRS-TR-03-011,25 October 2003.

[7] K. Fishkin and J. Lundell. RFID in healthcare. In S. Garfinkel and B. Rosenberg, editors, RFID: Applications, Security, and Privacy, pages 211–228. Addison-Wesley, 2005.

[8] M. Baard. RFID invades the capital. Wired News, 7 March 2005. Referenced 2005 at http://www.wired.com/news/privacy/0,1848,66801,00.html.

[9] C. Kocher, J. Jaffe and B. June . Differential Power Analysis,CRYPTO99

[10] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong Authentication for RFID Systems Using the AES Algorithm. In M. Joye and J.-J. Quisquater, editors, Cryptographic Hardware and Embedded Systems, CHES 2004, volume LNCS 3156, pages 357-370. Springer, 2004.

[11] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", in The First International Conference on Security in Pervasive
Computing SPC 2003, March 2003.

[12] Gildas Avoine and Philippe Oechslin "A Scalable and Provably Secure Hash-Based RFID Protocol", The 2nd IEEE International Workshop on Pervasive Computing and Communication Security Persec 2005, March 2005.

[13] Xingxin Grace Gao, Zhe Xiang, HaoWang, Jun Shen, Jian Huang and Song Song "An Approach to Security and Privacy of RFID System for Supply Chain", Proceedings of the IEEE International Conference on E-Commerce
Technology for Dynamic E-Business (CEC-East04), 2004.

[14] Martin Feldhofer Martin Feldhofer, An Authentication Protocol in a Security Layer for RFID Smart Tags, IEEE MELECON 2004, May 2004.

[15] P. Tuyls, B. Skoric, S. Stallinga, A.H.M. Akkermans, and W. Ophey. Information theoretical security analysis of physical unclonable functions. In A.S. Patrick and M. Yung, editors, Proceedings of 9th Financial Cryptography and Data Security Conference, volume 3570 of Lecture Notes in Computer Science, pages 141{155. Springer-Verlag, 2005.

[16] D. Johnson and A. Menezes. The elliptic curve digital signature algorithm (ECDSA). Technical Report CORR 99-34, Department of Combinatorics & Optimization, University of Waterloo, Canada, February 24 2000. http://www.cacr.math.uwaterloo.ca.

[17] M. Joye and S.-M. Yen. The montgomery powering ladder. In B. S. Kaliski Jr., CK. Kove, and C. Paar, editors, Proceedings of 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES), number 2523 in Lecture Notes in Computer Science, pages 291{302. Springer-Verlag, 2002.

[18] A. Juels. Strengthening EPC Tags against Cloning. March 2005. manuscript.

[19] A. Menezes, P. van Oorschot, and S. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997.

[20] P. Montgomery. Speeding the pollard and elliptic curve methods of factorization. Mathematics of Computation, Vol. 48:243{264, 1987.

Cryptography using Neural Network

[1]Himani Dua, [2]Abhay Shukla

HMRITM, Delhi, India
[1] himanidua1@gmail.com, [2] shuklaabhay256@gmail.com

***Abstract*—** Cryptography system helps in transformation ofinformation among authenticated users where there is no involvement of any third party using that information without that information with unauthorized access. This project implements encryption and decryption using neural network cryptography using AES key. The network construction will be generated solely on the parameters used in the training algorithm and the number of hidden neurons. In neural cryptography, both the communicating networks would receive an identical input vector(s), generate an output bit and are trained based on the output bit, the networks are to be synchronize to a state with identical time-dependent weights. This concept of synchronization by mutual learning can be applied to a secret key exchange protocol over a public channel which would be further used in cryptography. Earlier generation of secret key over a public channel used for encrypting and decrypting the given message using DES algorithm in neural cryptography was widely adopted. But, In this project we would using AES algorithm for key generation in neural cryptography. AES algorithm replaces the small key size generated by DES and also the Triple DES as it founds to be six times faster.

Keywords— Neural networks; Cryptography; Key Generation.

I. INTRODUCTION

With advancements in performance and requirements in technology, ciphers with better adaptation are proving to replace the weaker, slower and the aging algorithms for the current applications [1]. Algorithm for encryption can be symmetric or asymmetric. Symmetric encryption is fast. Due to its fast performance it is commonly used in e-commerce for transactions. Symmetric key algorithm(s) can be further classified as: stream ciphers and block ciphers. Block ciphers are mostly based on the idea by Shannon, that sequential application of confusion and diffusion, will obscure redundancies in the plaintext, where confusion involves substitutions to conceal redundancies, and statistical patterns in the plaintext, and diffusion involves transformations (or permutations), to dissipate the redundancy of the plaintext, by spreading it out over the cipher text. DES and Rijndael are examples of algorithms based on this idea. AES (Advanced Encryption Standard) is an iterated block cipher which was selected by NIST as an international standard, and replaced DES. It is now the most widely deployed block cipher in both software and hardware applications [2]. AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around(permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix − Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). As seen above, Alice and Bob share the same secret key. Bob can use the key to encrypt any message before passing it over a public channel. Here unauthorized person can only see the result of the encryption, but do not know the method to decrypt it. Once Alice receives the message it can be decrypted using Alice's copy of the key, transforming it back into plaintext.

II. IMPLEMENTATION OF ALGORITHM

A. Neurak KeyEexchange Protocol

The mostly used protocol for key exchange between two parties A and B in the practice is Diffie-Hellman protocol. Neural key exchange, which is based on the synchronization of two tree parity machines, should be a secure replacement for this method. Synchronizing these two machines is similar to synchronizing two chaotic oscillators in chaos communications.

B. Tree Parity Machine

The tree parity machine is a special type of multi-layer feed-forward neural network. It consists of one output neuron, K hidden neurons and K*N input neurons. Inputs to the network are binary:

$$x_{ij} \varepsilon \{-1,1\}$$

The weights between input and hidden neurons take the values:

$$w_{ij} \varepsilon \{-T_1, \ldots, 0, \ldots, T_n\}$$

Output value of each hidden neuron is calculated as a sum of all multiplications of input neurons and these weights:

$$\sigma_i = sgn(\sum_{j=1}^{n} w_{ij} x_{ij})$$

Signum is a simple function, which returns -1,0 or 1:

$$Sgn(w) = \{-1 \text{ if } x<0,\ 0 \text{ if } x=0,\ 1 \text{ if } x>0.\}$$

If the scalar product is 0, the output of the hidden neuron is mapped to -1 in order to ensure a binary output value. The output of neural network is then computed as the multiplication of all values produced by hidden elements. Output of the tree parity machine is binary.

1. Protocol: Each party (A and B) uses its own tree parity machine. Synchronization of the tree parity machines is achieved in these steps: Initialize random weight values
2. Execute these steps until the full synchronization is achieved
    i. Generate random input vector X
    ii. Compute the values of the hidden neuron
3. Compute the value of the output neuron
4. Compare the values of both tree parity machines
    i. Outputs are others: go to 2.I
    ii. Outputs are same: one of the suitable learning rules is applied to the weights After the full synchronization is achieved (the weights wij of both tree parity machines are same), A and B can use their weights as keys. This methods known as a bidirectional learning. One of the following learning rules can be used for the synchronization:

Hebbian learning rule: It is the rule which is used to alter weights between modal neurons. Anti-Hebbian learning rule: This rule is based on reverse of Hebbians's rule, it is basically used in reduction of synaptic connectivity between neurons.

Random walk:It shows the walk series for further predictions and consistently predict the next value in the series.

Brute force: To provide a brute force attack, an attacker hasto test all possible keys (all possible values of weights wij). By K hidden neurons, K*N input neurons and boundary of weights L, this gives(2L+1) KN possibilities. For example, the configuration K = 3, L = 3 and N = 100 gives us 3*10253 key possibilities, making the attack impossible with today's computer power.

Learning with own tree parity machine: One of the basic attacks can be provided by an attacker, who owns the same tree parity machine as the parties A and B. He wants to synchronize his tree parity machine with these two parties. In each step there are three situations possible:

Output(A) ≠ Output(B)

None of the parties updates its weights.

Output(A) = Output(B) = Output(E)

All the three parties update weights in their tree parity machines.

Output(A) = Output(B) ≠ Output(E)

Parties A and B update their tree parity machines, but the attacker cannot do that. Because of this situation his learning is slower than the synchronization of parties A and B. It has been proven, that the synchronization of two parties is faster than learning of an attacker. It can be improved by increasing of the synaptic depth L of the neural network. That gives this protocol enough security and an attacker can find out the key only with small probability.

Other attacks: For conventional cryptographic systems, we can improve the security of the protocol by increasing of the key length. In the case of neural cryptography, we improve it by increasing of the synaptic depth L of the neural networks. Changing this parameter increases the cost of a successful attack exponentially, while the effort for the users grows polynomially. Therefore, breaking the security of neural key exchange belongs to the complexity class NP. Alexander Klimov, Anton Mityaguine, and Adi Shamir say that the original neural synchronization scheme can be broken by at least three different attacks—geometric, probabilistic analysis, and using genetic algorithms. Even though this particular implementation is insecure, the ideas behind chaotic synchronization could potentially lead to a secure implementation.

Permutation parity mMachine: The permutation parity machine is a binary variant of the tree parity machine. It consists of one input layer, one hidden layer and one output layer. The number of neurons in the output layer depends on the number of hidden units K. Each hidden neuron has N binary input neurons. The weights between input and hidden neurons are also binary. Output value of each hidden neuron is calculated as a sum of all exclusive disjunctions exclusive or) of input neurons and these weights. The function θ N(x) is a threshold function, which returns 0 or 1. The output of neural network with two or more hidden neurons can be computed as the exclusive or of the values produced by hidden elements. Other configurations of the output layer for K>2 are also possible

Security against quantum computers: A quantum computer is a device that uses quantum mechanisms for computation. In this device the data are stored as qubits (quantum binary

digits). That gives a quantum computer in comparison with a conventional computer the opportunity to solve complicated problems in a short time, e.g. discrete logarithm problem or factorization. Algorithms that are not based on any of these number theory problems, are being searched because of this property.Neural key exchange protocol is not based on any number theory. It is based on the difference between unidirectional and bidirectional synchronization of neural networks. Therefore, something like the neural key exchange protocol could give rise to potentially faster key exchange schemes.

III. METHODOLOGY

Cryptography using neural network would be working on the phenomenon of neural networks which would be generated by the help of inputs taken from the server and the client, these inputs would be decided by the server and client on a public channel. After taking these input values, synchronization of these values takes place which would check if the values inputted on both sides are same or not because these values would be required in generation of a private key value. The inputs strength decides the key size that would be generated randomly but the values will decide the security strength of the key as in the key generated would be used in encryption as well as in decryption [3].

The following phases describes the working of cryptography using neural network. It is listed below:

A. Input Phase

Input of the parameters required for the synchronization of two networks, input values taken is the number of hidden layers units, the input layer units for each hidden layer unit, the range of synaptic weight values is done by the two machine A and B. The weight of the networks are initialized randomly using the input value of weight range. These values will decide the size and time for the creation of the key that would be used in the encryption and decryption of the data and also the key would be generated randomly for every process which would make this whole process of cryptography more secure.

B. Synchornization Phase

The initialized weight and inputs are used to calculate the output of each hidden neuron. The final output of the network is calculated using the outputs of each hidden neuron. If the final output value of the two networks are same, then synchronization takes place. If the final output is different, then it will return back to random initialization of weight. This process will take place until the final outputs become same for both the networks and the synchronization takes place which would make sure that both the machines A and B have the same private key on the public channel [4].

C. Key Generation for Encryption & Decryption

After completion of synchronization phase, the synaptic weights are same for both the networks now. So these weights would be used as secret private key which would be known to both the machines A and B which would help in sharing information on a public channel with only authorized and known machine as the secret key generated and used for encryption & decryption of the file to be shared between two networks is only known to the defined and connected machines sharing same secret key over a public network [5].

IV. CONCLUSION

In conclusion of this project we have implemented cryptography using neural networks which would be using key using AES algorithm. It will help in sharing information over a public channel using a secret private key that would be generated randomly and would only be known to the machines that are authorized machines which makes the whole network of transferring sharing of data secured.

V. FUTURE SCOPE

This research paper represents one of the application that is applied but as there is still a huge number of applications to study which can be further be taken in contrast of study and analysis. As this paper includes only rough sketch of what can be done using Neural Network by generation of key using AES key to encrypt and decrypt the data using symmetric key or private key. One can study and work upon more beneficial ideas to explore and increase the usability & feasibility so that each and every citizen of nation can use it widely like as e-commerce websites for shopping, delivering, transferring data.

The future work that may be done in this regard includes:

- Minimisation of the error function by improved methods
- Implementation of better training algorithms and network architecture
- Increasing the efficiency of training for the generalized cryptosystem

REFERENCES

[1] Lee,D "Hash Function Vulnerability function and Hash Chain Attacks" at 3rd IEEE workshop,2017,pp 1-6.

[2] Bradford,P.G; Gavrylyako,O.V "Hash chainswith diminishing ranges for sensors" at International conference,2014, pp 77-83.

[3] Al Housani,H;Baek,J; Chan Yeob Yeun "Survey on certificateless public key cryptography" at International conference,2011,pp 53-58.

[4] Al-Janabi, S.T.F.; Rasheed; M.A .-S "Public-Key Cryptography Enabled Kerberos Authentication" at Development in E-systems Engineering[DeSE],2011,pp 209-214.

[5] Feng Bao "A generic method of detecting private key disclosure in digital signature schemes" at 5th InternationalICST conference,2010,pp 1-5.

Data Integrity and Authentication in WSNs

Varun Tiwari

TIPS, GGSIPU, New Delhi
varuntiw1984@gmail.com

Abstract— This paper enlightens security features of WSNs (Wireless Sensor Networks) in terms of data confidentiality, data authentication and data integrity. The optimized security protocol has been designed to fulfil utmost prerequisite security features for WSNs. Efforts have been made not only to make secure protocol but energy efficient too. The Optimized Security Protocol (OSP) techniques are constituted to abide security requirements for message confidentiality, message authentication and message integrity. Further, proposed OSP design intends a solution that is secure as well as energy efficient. The Rabbit stream cipher has been the main focus for confidentiality provided by our OSP design. Also Rabbit based MAC function is being used extensively for the purpose.

Keywords— Wireless Sensor Networks**;** WSNs; **C**onfidentiality; **A**uthentications; **I**ntegrity; MAC**;** (Message Authentication Codes**.**

I. INTRODUCTION

The Wireless Sensor Networks (WSNs) is a collection of small battery powered devices that can sense various parameters like movement, pressure, temperature etc. These sensing devices collectively work in a networked environment to report the happening of various events.

Wireless Sensor Networks are now being deployed in environments that were previously thought to be impenetrable. Some of the application domains [1] include battlefield monitoring, wildlife monitoring, underwater deployment and vehicle tracking. Recent advancements in the field of computer and network security have been able to provide protection to various networks but WSNs have not generally been able to largely benefit from these advances. WSNs are unique in nature because they possess limited resources, yet they are deployed in environments that demand high level security. Research has shown that WSNs can be attacked by a wide range of methods, and each attack is unique and requires different techniques to counter the attack [2]. In such conditions the importance of a security protocol for WSN becomes twofold.

Designing a security framework for WSNs requires that we maintain the balance between resource requirement and functionality. So if a security framework is developed without maintaining this balance then it could render the network useless. Table 1 that shows the very limited resources available to a typical smart dust sensor.

TABLE 1:

THE RESOURCES OF A SMART DUST SENSOR [3]

CPU	**8 bit, 4Mhz**
Storage	8k instruction flash 512bytes RAM 512 bytes EEPROM
Communication	916 MHz radio
Bandwidth	10 Kbps
Operating System	Tiny OS
OS Code Space	3500 bytes
Available Code Space	4500 bytes

In this paper we have proposed a WSN security protocol for WSNs based on the Rabbit stream cipher. Keeping in view the importance of security requirements for WSNs, We have extended the Rabbit stream cipher that could previously handle only encryption and decryption of messages. The extension to the Rabbit framework has enabled us to provide a framework that provides encryption, decryption, authentication and integrity of messages. To provide the functions of authentication and integrity we have also modified the default packet format so our OSP provides the required functionality in a compact manner. In this paper we have adopted a comprehensive approach towards the development and deployment of a MAC based protocol for WSNs. Section II explains the security goals for WSNs based on which all security protocols are developed. Section III explains the security benchmarks of the OSP design. The security primitives employed by the OSP design are described in Section IV. Section V throws light on the eStream project and the Rabbit Stream Cipher for providing confidentiality in our OSP design. The key setup and trust establishment methodologies compatible with our OSP design are discussed in Section VI. Our OSP design, with details of its working is presented in Section VIII. Finally Section IX concludes our work with future directions.

II. SECURITY GOALS FOR WIRELESS SENSOR NETWORKS

For a security framework to be widely accepted and implemented it must fundamentally follow the following goals. Adherence to these security goals [4] should present a network with threat deterrence properties.

- Energy efficiency - Any security scheme designed for WSNs should be energy efficient. The scheme should provide security by consuming as little

resources as possible. Providing security at the cost of high resource consumption will cause resource depletion.

- No Temper Resistance - Wireless sensors are designed to be small in size and low in price. So the strength of the sensors actually lies in the fact that they are deployed in large numbers. Furthermore tamper resistance is normally not provided. Hence we need to ensure that a few faulty or compromised sensors should not render the network useless.
- Multiple layers of Defence - Such a scheme is also very beneficial for WSNs but it should only be employed in WSNs keeping in view their resource constrained nature and that multiple layers of defence do not drain the network resources.

III. SECURITY BENCHMARKS

OSP provides comprehensive security by guaranteeing confidentiality, authentication and integrity of messages, so that WSNs are protected against the threats that they are exposed to. The following section explains each of these security benchmarks and their importance in the proposed design.

A. Confidentiality

Confidentiality is at the core of all security activities. Confidentiality dictates that data is accessible by only those who it is destined for. This implies that any illegal or illicit mechanism of data access is a breach of the confidentiality principle. To provide confidentiality we can use techniques like authentication, access control and encryption. These techniques and many others are commonly implemented in conjunction with other techniques to further strengthen the system.

B. Authentication

Authentication in security requires that a person/agent/node is really who it claims to be. Authentication procedures ensure confidentiality and integrity of both the data and the system. Common authentication techniques include passwords, digital signatures and biometrics. Algorithmic techniques for ensuring authentication include Message Authentication Codes and their variants.

C. Integrity

Integrity is a concept that ensures that data can only be modified, replaced by authorized agents. Integrity deals with both the correctness and reliability of data. Integrity requires that the data being sent is complete, unmodified and entirely in its original form.

IV. SECURITY PRIMITIVES

OSP aims to provide confidentiality, authentication and integrity of messages by employing the following security primitives:

D. Cryptography

Cryptography is a widely accepted method of providing security in networks, however its success is entirely dependent on key management (key establishment, key regeneration, key exchange, and key withdrawal). Cryptography comes in two forms Symmetric Key Cryptography and Asymmetric Key Cryptography.

Symmetric Key Cryptography is based on the use of a single shared key. This key is shared between both the sender and receiver. Although this seems simple but the actual issue is the announcement of the key itself. To safely communicate the key there is need to establish a secure communication channel between both the sender and the receiver.

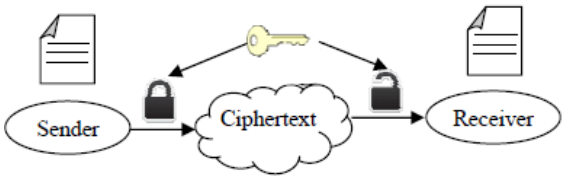


Fig. 1 Symmetric key encryption

On the other hand, Asymmetric Key Cryptography (Public Key Cryptography) resolves the issue of having a secure communication medium between the sender and the receiver by using two mathematically associated keys. The data is encrypted using a public key but it is decrypted using only the private key. Since the encryption and decryption process both employ two different keys therefore the entire encryption/ decryption mechanism becomes computationally complex.

"The problem with asymmetric cryptography, in a wireless sensor network, is that it is typically too computationally intensive for the individual nodes in a sensor network." Research [6, 7, 8] has proven that the above facts related to symmetric and asymmetric cryptography are generally true; however, the choice of an appropriate algorithm has a tremendous effect on the success of the system. Resource limitations in WSNs have forced researchers to consider unconventional schemes for providing security. Therefore in our MAC based Rabbit design we propose a fusion of both symmetric and asymmetric cryptography, employing the best features of both schemes keeping in mind the resource constraints. At the time of key establishment we use asymmetric encryption. Then we shift to symmetric key encryption to encrypt all data travelling between the sensor nodes.

E. Stream Ciphers

Stream Ciphers are symmetric key encryption schemes that employ a pseudorandom number generator which generates a random data stream which is typically XORed with the plaintext [9].Stream ciphers produce streams of data rather than blocks and these streams are random in fashion. As WSNs have inadequate RAM and processing capability, therefore, the obvious choice of ciphers is the stream cipher. Largely because, stream ciphers encrypt data bit by bit, thereby reducing bulk resource demand and produce a fast stream of data.

F. Synchronous Ciphers

WSNs are prone to transmission errors. These errors can be as a result of noise or they can be injected purposely by an adversary. Therefore, we need a state update mechanism that is resilient to transmission errors. Synchronous stream ciphers present a flexible mechanism of having an independent keystream generator. Using synchronous stream ciphers has the positive impact that the plain text has no impact on the keystream generator. In other words, the keystream generator does not operate in conjunction with the plaintext. If we use non-synchronous stream ciphers or block ciphers the situation is entirely different because an adversary can inject errors into the plaintext and the results would be devastating because each intermediate state (encryption and decryption) would also be entirely erroneous.

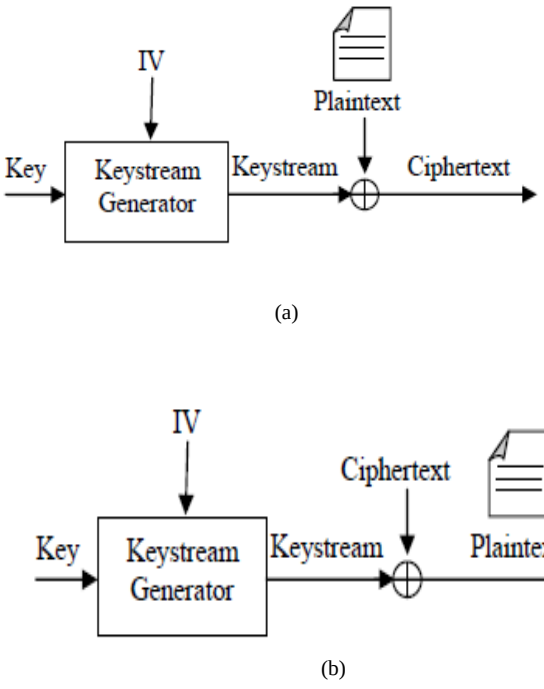


Fig. 2 Synchronous Stream Ciphers: (a) Encryption (b) Decryption

G. Message Authentication Code - MAC

Using encrypted messages is an effective way of providing the very basic level of security but to further prove the legitimacy of the plaintext using Message Authentication Codes (MAC) is a must. To produce a MAC the secret key and the message to be authenticated are processed by the MAC algorithm. The output obtained is conveniently called a MAC. The MAC works like a tag which is transmitted with the message. The receiver inserts the same key and the message to produce its own independent MAC. At the receiving end, if the senders MAC and the receivers calculated MAC match, then the authenticity of the sender is verified.

H. Initialization Vector

Neighbouring nodes in WSNs often exchange messages that are exactly identical or there are minor differences between the messages. In such situations, the use of an initialization vector (IV) can help in the generation of two broadly different cipher text even if two plaintexts are identical [10].

V. Rabbit Stream Cipher

Rabbit is a stream cipher that is part of the four stream ciphers that were finalized for wide adoption by the eSTREAM project. The general purpose of the eStream project was to identify stream ciphers that could be selected based on high throughput, low resource requirement and the ability of being implementable in a resource constrained environment.

The eSTREAM project is composed of multiple phases and the finalized list of stream ciphers is put forth after strenuous testing and investigation. The four finalized stream ciphers are Rabbit, HC, Salsa20 and SOSEMANUK. Essentially Rabbit is a 128bit stream cipher composed of a bit stream generator. The stream cipher has the ability to successfully mix inner state iterations and thus provide confusion and diffusion of the key stream.

VI. Key Setup and Trust Establishment

The key setup procedure determines how exactly the keys will be exchanged between the nodes of the network. WSNs are different in comparison to other usual networks, therefore a key exchange mechanism is needed that can be scaled to hundreds of nodes. Selection of an appropriate keying mechanism is based on the amount of resources available and the level of security required. Fundamentally there are three keying mechanisms namely network wide key, group key and per link key. In WSN any of the above key distribution techniques can be employed. Before a key distribution technique is selected we must compare the pros and cons of each and in the end the advantages should outweigh the disadvantages.

A single network wide key can be used, but it would compromise the network in case there is a security breach. On

the other hand, it is easy to deploy because a single key will be shared between all nodes. Moreover, upsizing and downsizing the network is very simple.

A group key can also be used that allows the sharing of a single key between a logical group of sensors. In the event of a security breach only the specific group is affected. The inherent disadvantage of this scheme is that it is more complex to deploy as compared to a network wide key. In per link keying, keys are deployed on per link basis.

In per link keying, in case of a security breach, only a single link is compromised; but based on the complexity and frequent resource demand this scheme fails for a resource starved environment. A single link key has better attack deterrent properties. Bringing down a single node does not result in the failure of the entire network.

VII. Design of OSP

The above discussed security primitives form the foundations of our proposed OSP. With the proposed OSP design we aim to improve the security and performance properties thus providing confidentiality, authentication and integrity. We propose an optimized security protocol for WSNs hence called OSP which provides confidentiality, authentication and integrity in WSNs. Due to the restrictions imposed on WSNs the major objective of OSP is to design a comprehensive security model while minimizing the cost effect of the following:

- Minimizing the cost incurred in communicating the encrypted packet.
- Minimizing the code space required for performing calculations.
- Minimizing the computation overhead in performing various cryptographic procedures.

A Confidentiality : Rabbit

Rabbit is exclusively designed for an environment where there is limitation of resources. This makes Rabbit very suitable for WSNs. Rabbit can provide both security and efficiency with its lightweight algorithm. Therefore our proposed OSP design rests on the Rabbit stream cipher coupled with an optimized packet format for providing confidentiality of messages in WSNs. The Rabbit algorithm is initialized by expansion of 128bit key into eight state variable and eight counter variables. The key and IV is inserted and four rounds of the next state function are performed to reduce the correlation between the bits of the key, IV and state variables. The next state function effectively and repeatedly jumbles up the bits so that no apparent pattern is visible. The keystream generator uses the same components to diffuse the state and counter variables.

B Packet Format

To ensure that Rabbit does not consume unnecessary resources and network bandwidth we have designed our own optimized packet format that is based on a few fields of the current TinyOS packet format with some additional fields to support our security solution. The fields common to TinyOS are dest address, AM and length. The fields Src, Ctr and MAC are appended in addition to the TinyOS header fields.

Dest (2)	AM (1)	Length (1)	Src (2)	Ctr (2)	Data (0...29)	MAC (4)

(a)

Dest (2)	AM (1)	Length (1)	Grp (1)	Data (0…29)	CRC (2)

(b)

Fig. 3 Packet Formats: (a) OSP packet Format (b) TinyOS Packet Format

The first three fields namely dest, AM and length are kept unencrypted so that they can be readily accessed by the receivers. If the fields are kept encrypted then each receiver would first have to decrypt the packet to check if it is the intended destination. The active message (AM) type is comparable to a port number in TCP/IP. It specifies the exact handler function that can extract and interpret the message on the receivers end. The TinyOS packet uses the group field which is a unique identifier for a group of motes participating in the network. Only those motes can communicate with each other that have the same group ID. In our proposed design we are not using the technique of network segmentation instead we use sensor to sensor communication, therefore the group field has been removed and a source field is included that identifies the sender of the message.

C. Authentication and Integrity: MAC

Rabbit was fundamentally designed to perform encryption, but to ensure comprehensive security only encryption is not enough. Authentication and integrity ensure that the message being received has not been attacked during transit and it also verifies the fact that the packet was sent by an authenticated party. In the absence of authentication, messages under transit are susceptible to cut-and-paste attack leading to severe consequences because in the absence of authentication there is no integrity.

The original TinyOS packet format uses the CRC instead of a MAC. It has been proven that CRC is a primitive mechanism for providing the very basic modification protection. The basic purpose of a CRC is to detect transmission errors and the mechanism fails to detect any sort of modification attacks. Therefore we promote the use of MAC because its advantages greatly outweigh the advantages of using a CRC. A MAC is able to protect even those fields in

the packet that are unencrypted. The MAC further protects the packet/data from tampering, truncation and other malicious modifications. Furthermore, besides providing the obvious security features the MAC can also

detect transmission errors. So just at the expense of two additional bytes our proposed OSP provides protection against a wide range of attacks and errors.

D. IV Format

To reduce the amount of resources consumed in providing encryption, authentication and integrity our IV is based on the fields proposed in our OSP optimized packet format. This method reduces the data cost and the processing costs emerging from the creation and use of an independent IV. The IV is extracted from the header fields in the optimized OSP packet and sent unencrypted to the receiving party. No independent initialization vector is ever sent from one node to another, this reduces the overhead of sending an independent IV from other nodes in the network. The IV format for our proposed OSP is as follows:

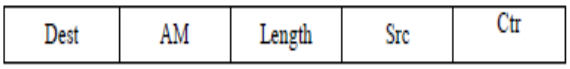


Fig. 3 IV Format

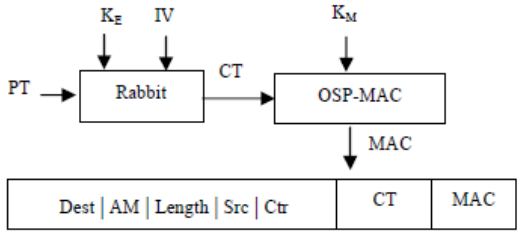
The unique combination of Src and Ctr fields ensures that each node can send at least 216packets before there is a global repetition of an IV value.

E. Next-state Function

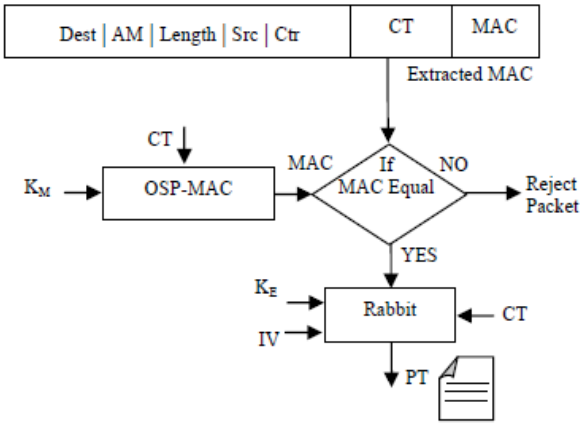
The next-state function [11] lies at the heart of the Rabbit algorithm because this function plays its role in key setup and keystream generation. The next-state function uses eight counter variables and eight state variables to produce a 128-bit key. The next-state function operates such that after a single iteration a single key bit has affected all the eight state variables. This illustrates that the next-state function is effective in providing diffusion and non linearity which prevents guessing based attacks.

F. OSP Design

To send an authenticated packet the sender needs to compute the MAC on the packet with an agreed Km and the packet is sent to the decrypting party. OSP is designed to provide encryption, authentication and integrity in WSNs. The OSP makes use of the Rabbit Next State Function for computing the MAC. The design of MAC is based on the next state function because of its good diffusion properties. Furthermore making reuse of the next state function for MAC calculation saves the additional program space for a separate MAC algorithm.



(a)



(b)

Fig. 4 OSP Process Diagram: (a) Sending Party (b) Receiving Party

Upon receiving this packet a node can verify that the packet has not been malformed during transit. To verify a packet the receiver computes the MAC along with the agreed key Km and the IV extracted from the packet header. This MAC is verified with the MAC received in the packet. If the two MACs do not match then the received packet is discarded (or any other action). This MAC scheme is commonly referred to as encrypt-then-MAC approach [12].

VIII. Conclusion and Future Scope

In this paper we have presented an optimized security protocol for WSNs which provides confidentiality, authentication and integrity. Our proposed OSP is an effort to optimize the existing rabbit stream cipher and to provide greater security to WSNs. We have designed a new packet format by modifying the TinyOS and Rabbit packet format. The advantage of such a scheme is that we have a smaller packet size and we have been able to promote the reuse of fields in the IV. Since the initialization vector is actually extracted from the OSP packet, therefore, there is no need to independently transmit a separate IV, thereby saving the essential battery space. Furthermore, OSP uses the next state

function for the computation of MAC, hence we can reduce the space requirement for maintaining a separate MAC algorithm.

The protocol OSP also gives rise to several future directions. Firstly, we intend to simulate our proposed optimized Rabbit based security protocol in TinyOS and prove the authenticity of the proposed scheme and that the proposed scheme works upto mark. Secondly, another direction could be to implement our protocol on other embedded sensor platform.

REFERENCES

[1] C.F. Hernández, P.H. Ibargüengoytia-González, J.G. Hernández, J.A. Díaz, "Wireless Sensor Networks and Applications: a Survey", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, Pages 264 -273. March 2007.

[2] Hasan Tahir, Syed Asim Ali Shah, "Wireless Sensor Networks– A Security Perspective", 12th IEEE International Multitopic Conference, Karachi, pp. 189-193, December 23-24, 2008.

[3] Pister KSJ, Kahn JM, Boser BE, "Smart dust: wireless networks of millimeter-scale sensor networks". Technical report, UC Berkeley, 1999.

[4] Yee Wei Law, Paul J.M. Havinga, "How to secure a wireless sensor network", Published in Intelligent Sensors, Sensor Networks andInformation Processing 2005. IEEE pp 89-95.

[5] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey". Security in Distributed, Grid, and Pervasive Computing. Auerbach Publications, CRC Press 2006.

[6] G. Gaubatz, J.P. Kaps, B. Sunar, "Public key cryptography in sensor networks – revisited", 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), 2004.

[7] D. J. Malan, M. Welsh, M. D. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography", First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, IEEE SECON, 2004.

[8] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, P. Kruus, "Tinypk: securing sensor networks with public key technology", Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN '04), pp. 59–64, New York, NY, USA, ACM Press, 2004.

[9] Alex Biryukov, "Block Ciphers and Stream Ciphers: The State of the Art"

[10] Chris Carlof, Naveen Sastry, David Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Network". 2nd ACM conference on embedded Networked Sensor Systems (SenSys 04), November 2004.

[11] Martin Boesgaard, MetteVesterager, Thomas Christensen, ErikZenner, "The Stream Cipher Rabbit". ECRYPT Stream Cipher Project Report 2005/006.

[12] M. Bellare, C. Namprempre, "Authentication Encryption: Relations Among notations and Analysis of the Generic Composition Paradigm", lecture notes in Computer Science Vol. 1976, T.Okamotoed, Springer Verlag, 2000.

Water Quality Analysis using Arduino

[1]Mamta Tholia, [2]Srishti Gupta, [3]Manuhar Swaroopa, [4]Shreyas Piplani
EEE, MSIT, New Delhi, India
[1]mamtatholia@msit.in, [2]guptasrishti97@ieee.org, [3]mkswaroopa1996@gmail.com, [4]shreyaspiplani@gmail.com

***Abstract*—** There is a dire need of effective water quality control system in the residential areas and the demand is very high due to urbanization, wide scale pollution and population growth. Scarcity of safe drinking water poses a great challenge to development. Necessary and immediate steps have to be taken to overcome it. At the very first, we have to assess water parameters like temperature pH, turbidity, conductivity etc., as the variations in these values can provide insights about the presence of pollutants. The monitoring of the water standard is a complex process as it has several laboratory testing methods which is very tedious and time consuming. To reduce the time, we need to look for automated system, a testing equipment that can be placed in the river or other water bodies especially in the rural areas where situation of clean and safe drinking water is very vulnerable. So we have proposed Arduino based water quality monitoring system that monitors the quality of water in real time. It consists of different sensors which measures pH, temperature and turbidity. The measured values from the sensors are processed by microcontroller and the processed values are transmitted using GSM to the concerned authority.The controller accesses the information which is monitored by the use of sensors. The accessed data are controlled by the usage of Arduino controller. By using an IoT, the information is collected and the water pollution can be enquired, by a strict mechanism.

Keywords— pH; Sensors; Temperature; SMS.

I. INTRODUCTION

Water quality in rural areas is difficult to monitor due to lack of connectivity from different water laboratories. In other areas, location-based real-time water quality data collection is a tedious job and highly dependent on human intervention. The presented paper introduces a low-cost battery operated smart phone-based embedded system design to measure different water quality parameters in various remote locations. Developed system measures pH, total dissolved salt (TDS) and temperature of the water samples using off the shelf available sensors. Measured pH and TDS dataset have been used to derive other water quality parameters using standard mathematical relationships such as salinity, oxygen reduction potential and conductivity.In the 21st century, there are lots of inventions, but at the same time were pollutions, global warming and so on are being formed, because of this there is no safe drinking water for the world's pollution. Nowadays, maintaining pure supply of water to the people is getting more challenging day by day. In India mainly is big cities the municipality corporation use lots of chemical to purify the river water then supply that to the people. And we reserved that water without any test. And we also don't know the water is either safe for drinking or not. And now a day's water quality monitoring in real time faces challenges because of global warming limited water resources, growing population, etc. Hence there is need of developing better methodologies to monitor the water quality parameters in real time. The water parameters pH measures the concentration of hydrogen ions. It shows the water is acidic or alkaline. Pure water has 7 pH value, less than 7pH has acidic, more than 7pH has alkaline. The range of pH is 0-14pH. For drinking purpose it should be 6.5-8.5pH. Turbidity measures the large number of suspended particles in water that is invisible. Higher the turbidity higher the risk of diarrhoea, cholera. Lower the turbidity then the water is clean. Temperature sensor measures how the water is, hot or cold. Here we addressed this problem

II. PROPOSED PROJECT

Our goal is to develop a system for real time quality assessment for water health at residential places using Arduino. pH, Turbidity and Temperature sensors are used to gather the parameters necessary to monitor water health in real time. Following are the objectives of the proposed system:

- To measure various chemical and physical properties of water like pH, temperature and particle density of water using sensors.
- Send the data collected to a Raspberry Pi, show the data in display and send it to a cloud based Database using Wired/Wireless Channel.
- Trigger alarm when any discrepancies are found in the water quality.

The detailed block diagram of the proposed design is given in Diagram 1.

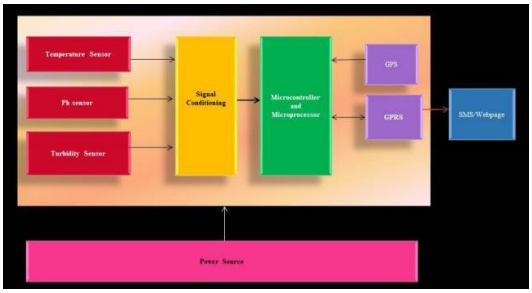


Fig.1. Block Diagram of proposed design

III. COMPONENTS

A Arduino

Arduino is an open-source platform used for building electronics projects. Arduino includes a physical programmable circuit board (often referred to as a microcontroller) and a piece of software, or IDE (Integrated Development Environment) that runs computer and is used to write and upload computer code to the physical board.

This platform has become quite popular for just starting out with electronics, and for good reason. Unlike previous programmable circuit boards, the Arduino does not need a separate piece of hardware (called a programmer) in order to load new code onto the board -- you can simply use a USB cable. Also, the Arduino IDE uses a simplified version of C++, making it easier to program. Finally, it provides a standard form factor that breaks out the functions of the micro-controller into a more accessible package.

Fig. 2. Arduino

B ADS1015

Analog to Digital Converter ADS1015 provides 12-bit precision at 3300 samples/second over I2C. The chip can be configured as 4 single-ended input channels, or two differential channels. Also, it even includes a programmable gain amplifier, up to x16, to help it to boost up smaller single/differential signals to the full range. We are using thiss ADC because it can run from 2V to 5V power/logic and it can measure a large range of signals and its super easy for use. It is a great general purpose 12 bit converter.

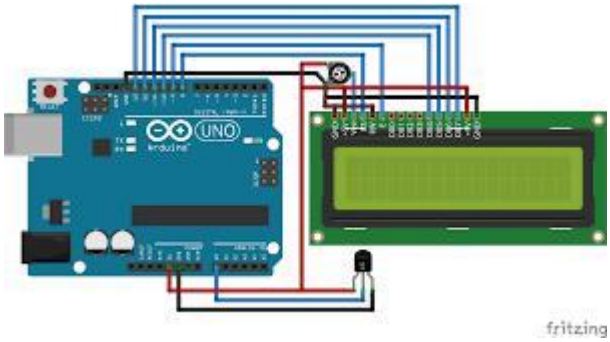


Fig. 3. nalog to Digital Converter

C. pH sensor

pH measurements are majorly conducted with pHsensitive glass electrodes, which have, in general proven efficient and accurate readings of pH. However, the behaviour of pH-sensitive glass electrodes often falls short of what precision is required. Even with the most careful treatment, the potential of cells containing glass electrodes often drifts slowly with time after such cells were placed in a new solution. Drift of cell potentials is an especially severe problem in investigations dependent on precise observation of small pH differences. Measurements involving cells with liquid junctions are subject to further uncertainties due to the dependence of liquid junction potentials upon medium concentration and composition and due to pressure changes in the system. The change in liquid junction potential (residual liquid junction potential) between test solution and standardizing buffer should be small or at least highly reproducible. In practice, systematic errors between many measurements suggest that the reproducibility of the residual liquid junction potential is often poor and that residual liquid junction potentials are dependent on the construction and/or history of the liquid junctions used in various investigations. Since pH fluctuations in marine waters are very small, an absolute accuracy of less than 0.1 pH units and a resolution of at least 0.01 pH units is required. For an assessment of the CO2/CO3 systems even a higher accuracy is necessary.

Fig. 4. pH Sensor with its electrode

D Turbidity Sensor

Turbidity is defined as the reduction of transparency of a liquid caused by the presence of undissolved suspended matter. The origin of the particles found in seawater can be mineral (such as clay and silts) or organic (such as particulate organic matter or living organisms like plankton). Turbidity is not, however, a direct measure of suspended particles in water, but a measure of the scattering effect such particles have on light. Turbidity sensors measure the amount of light that is scattered by the suspended solids in water. As the amount of total suspended solids (TSS) in water increases, the water's turbidity

level (and cloudiness or haziness) increases. Turbidity sensors are used in river and stream gaging, wastewater and effluent measurements, control instrumentation for settling ponds, sediment transport research, and laboratory measurements.

Fig. 5. Turbidity Sensor

E. Temperature Sensor

LM35 is a precision IC temperature sensor with its output proportional to the temperature (in oC). The sensor circuitry is sealed and therefore it is not subjected to oxidation and other processes. With LM35, temperature can be measured more accurately than with a thermistor. It also possess low self heating and does not cause more than 0.1 oC temperature rise in still air.

The operating temperature range is from -55°C to 150°C. The output voltage varies by 10mV in response to every oC rise/fall in ambient temperature, i.e., its scale factor is 0.01V/ oC.

Fig. 6. emperature Sensor LM35

IV. IMPLEMENTATION

In this system it makes use of four sensors (Turbidity, temperature, pH, conductivity) and the Arduino controller connected with internet of things. The Processing module microcontroller, and the transmission module GSM. The four sensors capture the data in the analogy signals. The ADC converter which converts the four signals information's into the digital format. The digital signals are passed to the Arduino controller which is together with the transmission module. The microcontroller in Arduino will examine itself and course the digital information, and here the available GPRS/GSM module is for next communication in the channel, the GSM model will send the water quality factors to the smartphone/PC by the SMS, which can be viewed on the LCD. Microcontroller in the Arduino accepts the information and processes the information which are collected from the sensors to the Web page via GSM module. With the help of coding the transmission is performed. The Embedded-C language is used for writing the code and Keil u vision software is used to simulate the program. For C programming we have used evaluation version of MDK-ARM v4. A software tool called Flash Magic is used for burning the. Hex files to NXP Controllers.

System Design : The water quality monitoring system employs sensors such as pH, temperature, Electric Conductivity (EC) and turbidity to get the data parameters. These sensors are positioned in the water will analyse the quality of the water resources. The verified content is used to prophesy the quality of water. The analysed data is processed through the microcontroller in the Arduino module and transferred through the GSM/Wi-Fi module using the data communication module to the central server. By giving a user id and password to the user they can view the data which is collected, processed, transmitted and analysed. The collected data is displayed in real time. The microcontroller in the Arduino is based on supporting the embedded trace & emulation through real time. It also supports the high speed flash memory in the embedded system. Hence the size is considered as the main requirement for the point of scaling applications and for controlling the access provided to the consumers it is good to use and it also consumes less power. It also suitable for providing the low resolution image with high processing power and by providing the protocol modifiers for communication in soft modems & in communications and providing paths with large buffer size. The Wi-Fi or GSM module used is merely low cost with chips in it. The wireless local area network provides service for offloading the other processor applications with Wi-Fi network functions or it also can host the various applications. The applications in this boots up from the external flash directly during hosting. Due to its integrated cache, the memory requirement is minimized and the system performance has been improved. Based on the type of interfaces like the UART interface or the CPU AHB bridge design, the microcontrollers can be accessed with the wireless internet access, it can be done when the Wi-Fi adapter works similar to the WiFi module. To send and receive data in Ethernet buffers, the Wi-Fi module uses the transceiver(Tx/Rx) which is in serial format. In the Wi-Fi module to change and query the configurations of Wi-Fi, serial commands are used. For the communications between a Wi-Fi module and the microcontroller it requires only two wires for the transmission and reception. Making the code very light weighted it allows the microcontroller to perform offload Wi-Fi related tasks on the module. To build an Internet of Things applications very easy, SPI and UART interfaces are addressable over the Wi-Fi module. To connect the TCP connections which is open and the Wi-Fi network we use the AT commands. The open TCP connections do not need any protocols like TCP/IP stack running in the microcontroller. The factors can be pushed to the internet (server) by the regular connections to the microcontroller.

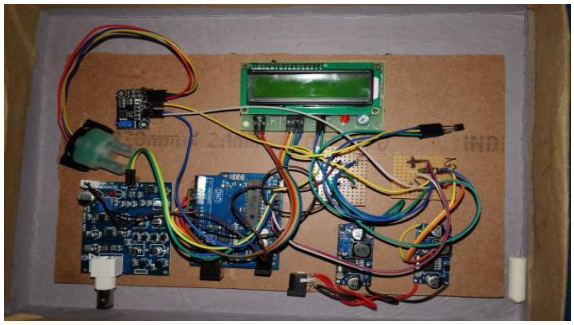


Fig. 7. System Design

V. RESULT

Water parameters are collected from the different set of samples. Then this data is displayed on LCD Collected data is forwarded to the server PC with GUI .From prior testing, a threshold value (range of values) is defined for the monitoring of pH, turbidity and conductivity of water. Depending on whether the average of the values obtained is less than or greater than the defined threshold, we get to know whether the water is acidic or basic, conductivity is high or low, is the water pure or impure and hence if it is suitable or not for the specific purpose. This system monitors the above mentioned parameters and finally when all check have been completed, its sends the information or data as an SMS to notify the authorized personnel. To determine the quality of water, the pH sensor and EC sensor is put into a container which is filled with tap water and 3-4 drops of acidic is mixed to it. when the pH of water is still around 3 - 4.5 range then the water is acidic in nature. And the surrounding temperature still between 32 to 34 degrees. The waters conductivity is 7 to 9 micro Siemens/centimeter. The total Dissolved Solids are 0.67*electrical conductivity which is measured from the graph.

VI. CONCLUSION

Monitoring of real time quality of Water from reserve tank of house and colony makes use of PH, turbidity and temperature sensor with Arduino and existing Cloud system for data analytics. The system can monitor water quality automatically and sends SMS so that necessary steps can be taken to prevent any health hazards if the water quality is at dangerous level. Also, it is low in cost and does not require people on duty. So, the system is likely to be more economical, convenient and fast. The system has good flexibility. Only by replacing the corresponding sensors and changing the relevant software programs, this system can be used to monitor other water quality parameters. The operation is simple. The system can be expanded to monitor hydrologic, air pollution, industrial and agricultural production and so on. It has widespread application and extension value.

REFERENCES

[1] Encinas, Cesar, et al. "Design and implementation of a distributed IoT system for the monitoring of water quality in aquaculture." 2017 Wireless Telecommunications Symposium (WTS). IEEE, 2017.

[2] Vijayakumar, N., and R. Ramya. "The real time monitoring of water quality in IoT environment." 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS). IEEE, 2015.

[3] Geetha, S., and S. Gouthami. "Internet of things enabled real time water quality monitoring system." Smart Water 2.1 (2016): 1.

[4] O'Flynn, Brendan, et al. "SmartCoast: a wireless sensor network for water quality monitoring." 32nd IEEE Conference on Local Computer Networks (LCN 2007). IEEE, 2007.

[5] Banna, Muinul H., et al. "Miniaturized water quality monitoring pH and conductivity sensors." Sensors and Actuators B: Chemical 193 (2014): 434-441.

[6] Page, Daniel. "Remote monitoring system for water." U.S. Patent Application No. 10/887,404.

[7] Ramos, Pedro M., et al. "A four-terminal water-quality-monitoring conductivity sensor." IEEE Transactions on Instrumentation and Measurement 57.3 (2008): 577-583.

Yojana Access: All schemes on one click

[1]Smriti Bhardwaj, [2]Namrata Mishra, [3]Ramneek Kalra
CSE, HMRITM, Delhi, India
[1]smritibhardwaj01@gmail.com, [2]namratta10@gmail.com, [3]kalramneek@ieee.org

***Abstract*—** In a developing country like India, it becomesmandatory that every underprivileged member of the country is aware of the various schemes initiated by the government. Making use of the machine learning and web development, we propose an idea to develop an online portal that will serve as the direct link between the government and the citizens which is "Yojana Access". This portal will reduce the paperwork andthere will hardly be any need left to actually go on-site and take the survey in person. On the basis of the data collected the portal will be able to display nearly exact statistics by making use of machine learning algorithms whereas the web development will help us create an interactive interface for the portal. Improving the communication between the government and the citizens is one of the major assistances that this portal will provide. Besides that, we will be able to fight poverty in a strategic manner. Through this portal we will be able to convey the different schemes to the citizens by attaching a link to these schemes in the portal. This will be another step towards the making of digital India and towards reducing corruption by removing the third party/mediators.

Keywords— Machine Learning, Web development, Digital India.

I. INTRODUCTION

Yojana access is a way to bridge the gap between thegovernment and the citizens. As India is a developing country, but we are well aware of the fact that we have a long way to go in order to transform into a developed country. The biggest barrier is the lack of communication between Govt. and citizens because of the involvement of mediators.

Why not remove the third party and create a direct medium of contact? This is where our proposed model of web application comes into play. **Yojana access** will not only layout the different schemes initiated by the government to the public, but it will help our citizens to check the statistics of the situation going to arrive in the future.

Currently, there is an existing portal, "MyGov" that communicates the different schemes of government classified by the jurisdiction. [1] Our model is to widen the scope of this classification. Besides jurisdictional classification we propose on making a region-based classification which will give us a better analysis of any country across the world with minor back-end changes and about the measures to improve it. Based on the schemes, the web application will survey the citizens and will develop the stats of forthcoming conditions, as explained stated in [2] that we can use different Machine Learning Algorithms for Predictive Analysis. For instance, let's take below scenario under which government is facing problems in analyzing data due to large volume: ***Scenario 1:*** Let us suppose that there is a village say,Hamidpur on the outskirts of Delhi where the natives are suffering from various issues but they do not have the medium to inform the officials/government. The natives are suffering from undeniable problems like water shortage, lack of electricity, health and sanitation and other unforeseen problems.

One day a group of few students from a nearby college went there with the motive of getting a rough estimate about all the complications the villagers face in their day to day lives on a sheet of paper. This survey was organized by the government where various institutions were given slots of 4 to 5 villages and then the colleges assign few students to collect data and in return, they get credit scores. Fortunately, Hamidpur locals had the opportunity this time.

The students worked strenuously for 5 days where they went to each and every household simultaneously filling and collecting data about all the whereabouts. The bulky papers were contributing towards the difficulties they were facing.

After collecting all the complaints/data the documents were dispatched to the government office. However due to large number of files from different places stacked one upon the other, it became quite impossible to read each and every complaint due to which solution, analysis, future predictions could not be found so the purpose diminishes and hence affecting the transparency.

Hence with the advancement in technology we need a portal that not only focuses on getting a solution but also provides quick useful insights.

This will reduce paperwork and the data will be more secure and organized.

The agenda of this research model is to establish a platform where one can survey the issues faced by the general public and deliver statistical results & predictions for the same. The problem statement describes the representation of issues faced by public in a statistical format, making use of web development and machine learning algorithms. Such that the user can check the statistics of future conditions about water supply/electricity supply and a lot of other conditions. The whole research study and related work can be summarized under the following sections.

II. METHODOLOGY

Before emphasizing the methodology let's have a look on the basic architecture of Yojana Access which can be used to calculate the statistics of future conditions.

A Algorithm for Yojana Access

One can review the algorithm that we are hereby using in the implementation of this model. This is the very basic flow Algorithm:

1. Initially, user (Citizen/Govt. Admin) will login in its dashboard by selecting "Login | Dashboard"
2. User will enter "Aadhaar Card Number" or will Select Social Contacts to link

2.1 If (Entered Aadhaar Card is equal to Aadhaar Database Entry) then:
Login Successful
Goto Step 3

2.2 Else
Login Unsuccessful
Go Step 4

3. After accessing the Dashboard, Valuable Pie Charts expressing State/District/Country wise data with prediction of next weeks or months for any problem that Citizens are facing on the basis of Real-Time Data Prediction Technique.
4. Check if User is registered or not using Firebase Authentication Database on the Cloud.

4.1 If (User is not registered) Redirect to Registration Page Goto Step 2

4.2 Else
Goto Step 2

5. Exit

B Software Architecture

Now, let's discuss the software architecture of the portal. We require data to analyse. How will we actually collect that data. This is where, the web interface will help us build a platform that will directly interact with the end user and fetch the data from the user and send it to the backend server.

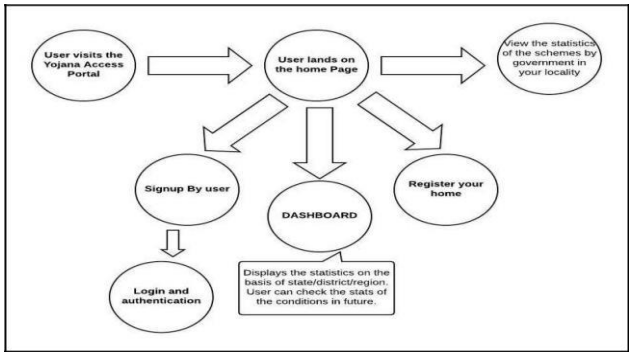


Fig. 1. Symbolic Block Diagram of Yojana Access web portal

The above symbolic block diagram, display the rough architecture of the web portal along with its features. The website is a multi-page and consists of the following pages.

- Index/Home page
- Dashboard
- Signup/Login
- Register your home

This was all about the outline of the web application but for developing an amazing UI, a lot of other things are to be taken into consideration. The fundamental on which this portal will operate is the data retrieved from the user. And to store the data we need database. The database that we are using in this system is Firebase Cloud Realtime Database.

As depicted in [3], Firebase is the most secure and tested platform for sharing and creating own private data store. But, before database, let's have a look on detailed Use case as depicted by Figure. 2.

We have considered 3 actors who are the direct stakeholders of this web application.

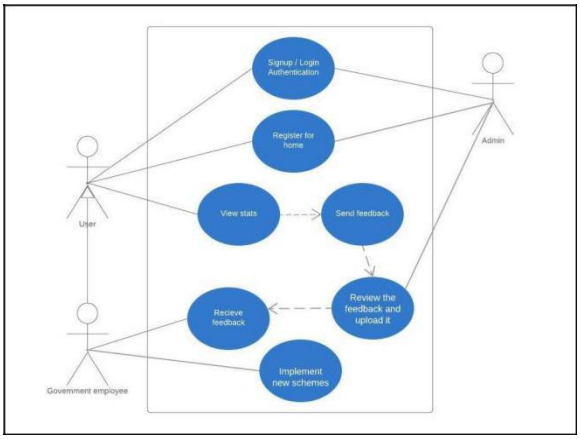


Fig. 2. Use case diagram for the data flow

As depicted in [3], Firebase is the most secure and tested platform for sharing and creating own private data store. But, before database, let's have a look on detailed Use case as depicted by Figure. 2.

We have considered 3 actors who are the direct stakeholders of this web application.

End user - End users, are the citizens who can sign upand login, can view the different schemes of the ruling body for their locality and view the statistics of upcoming conditions in the future.

Admin - Admin has the authority to handle and accesseach and every feature of the website including the database. Admin is responsible to handle the technicalities of the website.

Government Employee - The role of the government employee will be to consistently upload the schemes and take feedback from the users.

- Login/ signup: As the user visits the website, he/she will have to sign up followed by the login and authentication.
- Register for home: The user can begin registering their home.
- View stats: The stats are accessible to every actor and can be filtered on the basis of jurisdiction and region.
- Send feedback and suggestions: It is not just limited to viewing stats and schemes. The user can also provide his/her feedback and suggestions for the enhancement of the website and schemes.
- Review feedback and upload it: It will be the responsibility of the admin to review the feedback for any spam or inappropriate comment and upload it.
- Feedback Notifier: The government employee andthe admin will receive the feedback and can operate accordingly.
- Implement/upload new schemes: The governmentemployee has the authority to upload new schemes being initiated by the government

For registering home, we require a database with a table with the following attributes:

- Id
- Village name
- Gram Panchayat
- Ward Number
- Block State
- Personal details, etc.

Fig. 3. Depiction of "Register your home" | Yojana Access

As you can observe in this screenshot, we have created a dynamic interface to fetch the data from the user and send it to the backend server using firebase real-time database.

Here is a depiction of the flow of data form the front end to the backend and vice versa.

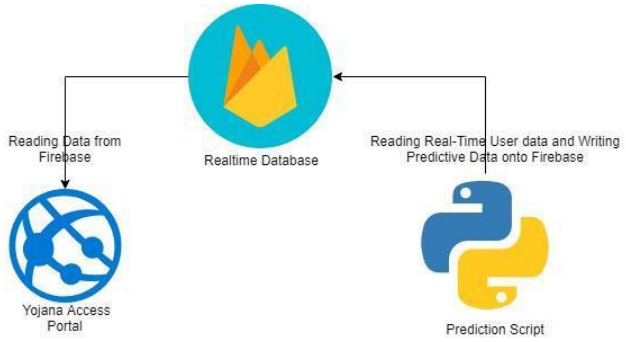


Fig. 4. Back-End Functioning Depiction

This is our interpretation of the data flow. This is how the data will flow from the backend server where the data will be analyzed and predicted, to the front end via real-time database.

C Implemented Work

Here is a depiction of the implemented work

Here is a depiction of the implemented work.

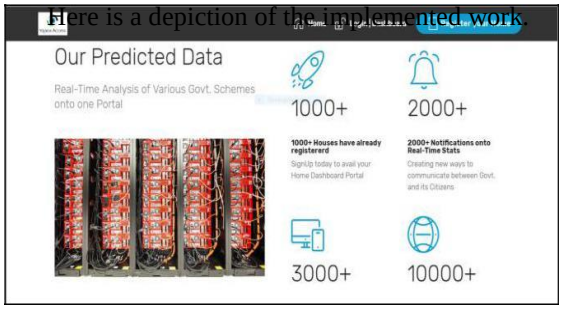


Fig. 5. Depiction of Home | Yojana Access

III. FUTURE SCOPE

We curated this research paper with the mindset of providing each and every individual an approach through which they can communicate with the government where web application will be the interface for communication. This is a trivial step which will show great results in succeeding years. Later, we will implement this in the form of a mobile app that will be available on iOS, Android and Windows stores. Also,

since the problems never cease to exist therefore this software will be developed in such a manner that it will be able to modify itself from time to time and which show valuable results as we are using the latest technologies which will predict and help in solving future problems. Also, we will make different for different yojanas so that it will be able to cover everyone on a large scale.

IV. Conclusion

This systematic study on various schemes and their fruitful enactment in the administration through the making of portal will be worthy if accounted on a positive note by the government. By making this portal we will be able to focus on the following points:

- Less paperwork
- More efficient
- Transparency between people and government
- All root problems will be covered.
- Involvement of mediator/external agents will also decrease.
- No need to search different websites as everything will be available on a single platform.
- It will help in digitizing India.

References

[1] "MyGov: PM Narendra Modi launches website for citizens".india.com. India Webportal Pvt Ltd. Retrieved 12 August 2014.

[2] M. Günay and T. Ensarı, "Predictive churn analysis with machine learning methods," *2018 26th Signal Processing and CommunicationsApplications Conference (SIU)*, Izmir, 2018, pp. 1-4.

[3] V. Mutiawani, S. Rahmany and T. F. Abidin, "Anti-theft Vehicle Monitoring and Tracking Android Application Using Firebase as Web Service," *2018 International Conference on Electrical Engineeringand Informatics (ICELTICs)*, Banda Aceh, 2018, pp. 72-77.

Volume-4, Issue -1
Jul – Dec, 2018

ISSN : 2581 - 4125

Contents

HMR Institute of Technology & Management
(Affiliated to Guru Gobind Singh Indraprastha University, Delhi)
Plot # 370, Hamidpur, Delhi – 110036
www.hmritm.ac.in editor. journal@hmritm.ac.in