International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 6, November- December 2017 ISSN 2278-6856

A Hybrid Approach to Secure RFID/Sensor Based SCM Systems

Belal Chowdhury[1], Subhasis Mukherjee[2], Nasreen Sultana[3],Maynul Hasan[4]

[1,2]School of Information Technology& Engineering, Melbourne Institute of Technology
288 La Trobe Street, Melbourne 3000 Australia

[3]Monash Health, Dandenong Hospital.
135 David Street Dandenong VIC 3175

[4]Hospitality Industry

Abstract: ***The use of RFID (Radio FrequencyIdentification) technology can be employed for not onlyreducing company management costs but also to track eachcontainer, pallet, case, product being manufactured,shipped and sold, uniquely to increase more visibility andaccountability in the supply chain.They connect supply chain stakeholders (i.e., suppliers, manufacturers, wholesalers/distributors, retailers and customers) and allow them to exchange data and product information. We outline a RFID model for the Pharmaceutical Supply Chain Management System as a case study to provide accurate, real-time information on products as they move to the value chain and by automating related business processes.***
Despite these potential benefits, security issues are the key factor in the deployment of a RFID-enabled system in the global supply chain. This paper proposes a hybrid approach to secure RFID transmission in Supply Chain Management (SCM) systems using modified Wired Equivalent Encryption (WEP) and Rivest, Shamir and Adleman (RSA) cryptosystem. The proposed system also addresses the common loophole of WEP key algorithm and uses a hybrid encryption based approach to solve the problem.
Keywords: WEP, RSA, SCM, RFID and PSCMS

1. INTRODUCTION

A supply chain is a network of facilities (e.g., retailers, wholesalers, transporters, storage facilities, manufacturers and suppliers)that encompasses all activities and information flow necessary for the transformation of goods from the raw material to finished products, and the distribution of these finished products to the end user [11]. Supply chainmanagement (SCM) refers to a set ofapproaches utilised to efficiently integrate and coordinatethe materials, information and financial flows across thesupply chain, so that product is supplied, producedand distributed at the right quantities, to the rightlocations, and at the right time, in the most cost-efficientway, while satisfying customer requirements [20]. SCM can connect all participants of a value chain in an efficient network of relationships and transactions that can decrease costs, improve customer service, improve the enterprise's knowledge base, increase efficiency within the organisation and create barriers to entry for competing organisations [19].
Automatic identification and data capture technologies (such as barcodes) have been around since 20th century to identify and track marked items accurately as they move through the SCM. They can assist in the data aggregate, and transfer data to automated information systems. These technologies can be used toreduce administrative and logistics costs in the supply chain by improving data accuracy (eliminating errors), speeding the collection and transmission of data, and automating the entire data entry process more efficiently [1]. For decades, barcodes are conventional identification techniques that have been incorporated into supply chain management to identify products, and track their movement in the value chain.

Theemergence of RFID technology presents an exciting new opportunity to improve the way the industry captures and uses product data throughout the supply chain. RFID is an automatic identification and data capture technology, which can enable companies to automatically identify and track items in the supply chain. The origins of RFID technology date back to the 1940s, when the principles behind radar technology and the theory of reflected power, which constitute the basics of modern RFID, were being initially developed.The first RFID applications were used to identify friendly aircrafts (IFF System, Identification Friend or Foe) during the Second World War[28].In the 1970s, New York Port Authority introduced an RFID device used for toll collection. The 1980s became the decade for full implementation of RFID technology in areas like transportation, personnel (keyless) access, livestock, industrial and business applications, and through toll roads in various parts of the world specifically in United States and Europe. The 1990's were a significant decade for RFID due to the emergence of standards to allow systems to work together and wide deployment of the technology [2], [3]. While RFID applications used earlier are still around today, many more RFID applications have emerged since then.

Recent development in telemetric and mobile commerce makes RFID an integral part of everyday life. Many large companies such as Wal-Mart, Target, Mark & Spencer, Metro AG, Tesco and Carrefour seized the opportunity to optimize their supply chains with RFID technology, which is far more powerful than barcodes. In addition, they provide unique identification for each tagged unit whereas barcodes are identical for every unit of the same product [6]. The components of RFID technology are becoming smaller and smaller, less expensive and more effective.

Thus, applications of RFID in supply chain have increased substantially. Recent report predicts that the growth of RFID as from $1 billion in 2003 to $4 billion in 2008 to $20 billion in 2013 [27].There is a little doubt that RFID will become a pervasive technology in the future [21].

The main components of the RFID-based system are RFID tags (i.e., tiny chips), RFID readers and the enterprise's IT systems. Unlike barcodes, RFID technologies do not need line of sight and the tag (RFID) can be read without actually seeing it [4]. In addition, RFID tags read rate is much faster than the barcode system. They can do a limited amount of processing, and have a small memory of 1024 bits of storage. There are some advanced RFID readers that can read up to 60 different RFID tags at approximately the same time, while a barcode reader can scan only one item at a time [5]. RFID tags are very effective in being read a variety of substances and conditions such as extreme temperature, soil, dust and dirt, fog, ice, paint, creased surfaces, and other visually and environmentally challenging conditions, where barcodes technologies would be useless [6].Despite these potential benefits, security issues are the key factor in the deployment of a RFID-enabled system and imposes significant threat on overall profitability in the global supply chain [21]. This paper identifies, and examines these threats and proposes a hybrid approach to secure RFID-enabled SCM systems.

The rest of the paper is structured as follows: section 2 outlines the benefits of RFID technology in the SCM. Section 3 provides overview of RFID model for SCM. Section 4outlines the Security threats of RFID-enabled SCM systems. Section 5illustrates the analysis of RFID-enabled SCM systems security. This section also discusses on the existing and modified cryptographic algorithm for the security of RFID-enabled SCM systems. Section 6 outlines the problem to the hybrid technique and a proposed solution. Section 7 concludes the paper.

2. BENEFITS OF RFID IN SUPPLY CHAIN

SCM is the oversights of materials, information, and finances as they move in a process from supplier to manufacturer to wholesaler to retailer to consumer [11]. Electronic systems within the SCM could be classified into three main flows such as the *product flow, information flow and finances flow.* The product flow deals with the movement of goods from a supplier to a customer. The information transmits orders and updates delivery status. The financial flow deals with credit terms, payment schedules, and title ownership arrangements [12]. A SCM involves coordinating and integrating these flows both within and among to reduce inventory. Electronic supply chain activities cover everything from product development, sourcing, production, and logistics, as well as the information systems needed to coordinate these activities [11].

SCM encompasses not only domestic and international industry sectors but also suppliers. Supply chain managers are currently facing significant challenges in managing their supply chains [23]. Increasing global competition is putting pressure on supply chains to be cost effective, efficient and more proactive in order to gain competitive advantage in the market. There is a growing trend amongst businesses and governments in the developed as well as emerging economies such as China, and India to coordinate and increase collaboration in their governments, business activities and processes. Effective and well-planned electronic SCM systems within governments and industry provide opportunities to continuously improve operations both within and external to an organization [13]. In recent years, information technology (IT) is contributing a significant role in bringing opportunities and challenges to SCM and making it grow at an even faster pace. In the past few years supply chain players (e.g., wholesalers) are persistently struggling to get the right products to the right retailers at the right time [14]. According to the Federal Trade Commission, "every year, American merchants lose as much as $300 billion (US) in revenues because they've lost track of goods somewhere on the journey between factory and store shelf." Lost revenues are not the only concern in the supply chain; improving the productivity in transporting goods and securing the source of goods are also of concern to professionals managing the supply chain [30].

All these problems can be solved effectively by RFID technology and is likely to make the largest impact on SCM over the next decades. RFID technology can also stamp out counterfeit products such as drugs, fight terrorism, and at the same time help companies like Wal-Mart keep its shelves stocked [15].Once Wal-Mart identified RFID as a potential cost reduction technology, many companies began to use RFID to track product flow.Report shows that after the deployment of RFID technologies, Procter & Gamble and Wal-Mart simultaneously reduced their inventory levels by 70%, improved service levels from 96% to 99%. They also reduced administration costs by re-engineering their supply chains [29].

RFID is being used in SCM (e.g., in transit, warehouse, etc.) to identify inbound and outbound products in real-timeto increase efficiency in areas like retailers, hospitals, farmers, and public transport. They connect suppliers, manufacturers, distributors, retailers and customers and allow them to exchange product and trading partner data. As a result, companies can make substantial annual cost savings by reducing inventory levels and lowering distribution and handling cost, increased security and product integrity, and greater flexibility [7].

RFID-based systems in SCM use tiny chips (or smart tags) contain and transmit product or item information to an RFID reader, a device that in turn interface/integrate with company's IT systems for processing through wireless communication (i.e., air interface). The product

information such as product ID, manufacture date, price, and its distribution point can be written to the tag to enable greater product accountability and safety. Due to the larger amounts of data storage and capacity for interactive communication RFID technology is likely to increase more visibility and accountability in the supply chain. It is useful for governments, manufacturers, retailers, and suppliers to efficiently collect, manage, distribute, and store information on inventory, and business processes. A RFID technology can also automate workflow, reduce inventory and prevent business interruption in the assembly process. In the long term, RFID technology has the potential of helping retailers provide the right product at the right place at the right time thus maximising sales, profits and prevent theft. To be functional, an RFID technology must be integrated with various information systems along the supply chain management to provide a meaning to the data and to allow for information exchange of companies (e.g., healthcare, retail) using the technology. Despite these potential benefits and some clear advantages over bar coding, there are some security issues with implementing RFID-enabled system applications in the global supply chain.

3. RFID MODEL FOR SUPPLY CHAIN MANAGEMENT

We outline a RFID model for the Pharmaceutical Supply ChainManagement System (PSCMS)as a case study, which canhelp pharmaceutical companies by providing accurate, real-time information onproducts as they move to the value chain and by automatingrelated business processes is shown in Fig 1.

Figure 1. Pharmaceutical SCM System overview

The pharmaceutical industry relies upon the integrity ofmany forms of data throughout the process of drug trials,suppliers (chemical plants), manufacturers, wholesalers, andretail and/or hospital pharmacy. Drug packages only equipped with barcodes are not unique for each product and they are easy to copy. RFID tags, on the other hand, are unique for all items and significantly harder to copy or tamper with. By RFID tagging as well as tracking and identifying the drugs on an individual basis, the likelihood of a counterfeit drug to travel all the way to its final destination is reduced significantly.

The product flows of RFID-enabled PSCMS are shown in Figure 1. Each unique product/item tag can be passive, semi-passiveor active [8]. Passive RFID tags are used for bothreading/writing capabilities by the reader. They do not needinternal power (i.e., battery) as they are energized by thereader through radio waves and have a read range from 10 millimetresto almost 10 meters.PSCMS involves coordinating and integrating these flowsboth within and among pharmaceutical companies and many activities that are related to the movement of drugs.The movement process includes placing or retrieving drugs inand out, the storage area or transferring goods directly fromreceiving to shipping docks [5]. RFID readers are placed inthese receiving and shipping areas to read tagged items (e.g.,containers in the chemical plants) for each supply chainplayers (e.g., manufacturer). Chemical plants (i.e., suppliers)create raw materials and place them into containers or drums.A RFID passive tag is attached to each container to identify and serve as the data carrier. Information about medicament ingredients as well as a serial number and other essential product information are added to an RFID tag that is attached on the container or package of the drug. The drug package tag can contain information not only about its own origin, but also about the ingredients and the amount of each ingredient in the drug. The passive RFID tag (with ahigh frequency of 13.56MHz) antenna picks up radio-waves orelectromagnetic energy beamed at it from an RFID readerdevice (i.e., placed in the chemical plants shipping area) andenables the chip to transmit containers unique ID and otherinformation (if any) to the reader device, allowing thecontainer to be remotely identified.

The reader converts theradio waves reflected from the tagged container intodigital information then pass onto SCM's IT system forprocessing. The system then stores containers information intothe supplier database before sending them to the manufacturer.On receipt of the tagged containers, the manufacturer trackscontainers using RFID readers that are placed in drugs (e.g.,raw materials) receiving area, verify the quantity of drugsbeing delivered and combines raw materials to makepharmaceuticals (e.g., sleeping pills). Pharmaceuticals are thenplace into tamper proof bottles and tagged with RFID tags.RFID readers (i.e., placed in manufacturer's shipping area)track tagged bottles and record the inventory intomanufacturer back-end database. The tagged bottles are thenship to the wholesalers.The wholesaler tracks and records each bottle that isshipped from the manufacturer. The pharmaceutical (e.g.,sleeping pill) bottles are then ship to the retail or hospitalpharmacies.Pharmacists or stores are equipped with RFID readers toverify that the tagged pharmaceuticals received fromwholesalers originate from its purported

manufacturer. A RFID enabled PSCMS help pharmacists (both retail andhospital) to automate existing system, checkout, and inventoryand maintain their day-to-day activities very effectively andefficiently.

4. SECURITY THREATS OFRFID-BASEDSCM SYSTEMS

There are key security threats or issues that pose the major challenge with the deployment of RFID-enabled system in the global supply chain due to the wireless communication [22].Some of the challenges are as follows:

A. Privacy

Privacy issues loom as one of the biggestconcerns to the success of RFID implementation inSCM system. The rising concern about the humanbasic right of privacy argument can be compromisedby the emerging technology. In addition, privacy advocates express concerns that placing RFID tags in commonitems or products may continue to be tracked oncepurchased by consumers. One of consumer's seriousconcerns is that once they own items (e.g., sleepingpills from a retail pharmacy), they do not wantthemselves or purchased items to be tracked afterpassing the checkout [7].

B. Alteration of tag data

An attacker modifies, adds, deletes, or reorders tag's data, such as product serial number.Further with respect to Read/Write (reprogrammable) tags, unauthorized alteration of product data can be the possibility in the SCM system.

C. Denial of service

An attacker blocks or disables networked systems,preventing, delaying or limiting access from the authorised users in the supply chain.

D. Eavesdropping

An intruder intercepts communication between an RFID token and an authorized reader in a supply chain and can access sensitive tag information such as product ID, name, supplier, manufacturer, and so on.Eavesdropping on RFID readers is a major threat in SCM.

E. A brute-force or dictionary attack

An attacker attempts to discover a password by systematically trying every possible combination of letters, numbers, and symbols until discover the one correct combination that works.

F. Security of communication channel

Most of the security threats in SCM are attributed to the security of the communication channel between authentic RFID readers, and the tags through the air interface (i.e., wireless communication). A RFID tag reading occurs when a reader generates a radio frequency "interrogation" signal that communicates with the tag (e.g., a tagged container), triggering a response from the tag [8]. Unauthorized readers can trigger this response of revealing the product information such as drug ID or even misuse by hackers and criminals.

5. ANALYSIS OF RFID-ENABLED SCM SYSTEMS SECURITY

The communication between RFID reader and tagged items normally happens through an air interface (i.e., wireless communication) in the RFID-based SCM system. This makes the SCM system vulnerable to attackers. As a result, security is the key issue which presents a host of challenges for the successful implementation of RFID technology in the SCM. To address RFID security issues, we propose a separate security layer in the RFID-enable SCM system architecture. The security layer implements a modified cryptographic algorithm initially proposed by other researches [9].The researchers propose a common encryption technique is to use Rivest Code 4(RC4) algorithm implemented with WEP key to hide plain text during communication [26]. But the process is vulnerable to statistical attack provided enough cipher text is available from the wireless source [9], [10]. A recent advancement suggests that elimination of transmission of Initialization vector (IV) stops the application of statistical attack hence neutralize the threat [9][24]. However, this technique uses linear increment of frame sequence number and/or other network traffic information to replace IV. An unauthorized person may extract the same data from the wireless frames going back and forth and so use them to run a known attack to recover the WEP key and hence the successful breach of data secrecy.

5.1 Universal WEP key technology

WEP key exists for quite a long time and been exploited in a number of ways. The working principle of the universal WEP key system is shown in Figure 2. According to the WEP key algorithm, both IV and cipher text is transmitted together over the AIR [18]. The clear text format of IVs is proven dangerous as it can be used for the decryption of the cipher text, send along with it. Usually four different IVs derived from the plain text message itself are used by rotation in order to produce cipher text with the conjunction of the private WEP key.

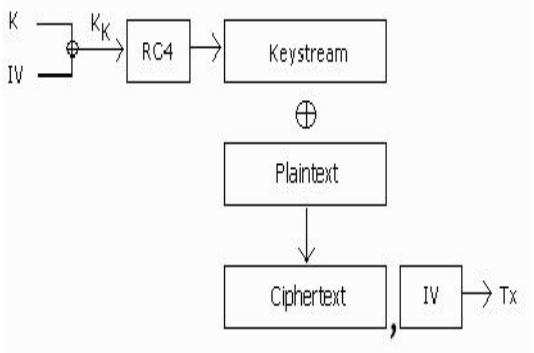

Figure 2. Universal WEP key generation and transmission

This repetitive nature helps a statistical model (attack method) to compare the IVs against captured cipher texts

and finally find out the WEP key provided enough IVs have been captured using authentication request message to the wireless card reader.

5.2 Related work in RFID-enabled SCM systems security using WEP technology

A different approach prescribes local generation of IVs in both transmitter and receiver in order to stop the transmission of IVs. Figure 3 shows this form of WEP key generation and transmission system.

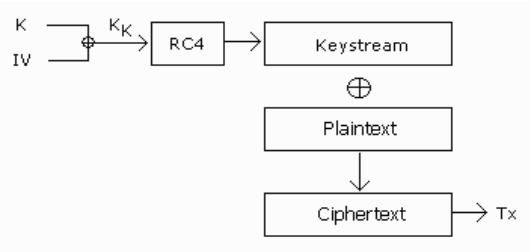

Figure3. Modified WEP key generation and transmission

The modified WEP key process defines that the IVs are not transmitted through the air [17]. It is generated instead using the different parameters of the network flow. A frame sequence number is such a parameter that can be used in a modified form as IVs. The incremental nature of such a property can be used to produce the repetitive IVs as well. However, the receiving end should be able to regenerate it before decryption of the actual data frame. Thus, it makes a fixed process of IV generation. As a result, if an attacker can obtain that series by trial and error method or any other means, rest of the decryption would be straight forward. Furthermore using the conventional statistical attack, the hidden WEP key can be found.

A recent paper suggested another approach to make a revolutionary change to the algorithm of the WEP key algorithm. Currently the RC4 algorithm is used within WEP to mix IV and plain text to generate encrypted bit stream. The new publication [25] proposes Elliptical Curve Cryptography (ECC) technique to replace RC4. However, this process demands a radical change in the hardware of all existing WEP key systems. The existing systems cannot be re used using this approach at all.

5.3 The proposed system

This paper proposes an RSA public key process to encrypt the IV data and send it over the air along with the cipher text. This encrypted IV cannot be used with the known attack techniques against WEP key encryption. It may be considered here that RSA algorithm is vulnerable to known-plaintext attack. Whereas in a given supply chain scenario the attacker has the least chance to find out the known plain text (The actual IV generated from the original data) to decrypt the cipher text made with RSA. The strength of the RSA algorithm makes it impossible to use brute force attack to determine the decryption key hence the IV in the form of plain text. In a supply chain, process products get scanned quickly and simultaneously. Therefore, a brute force attack is not feasible in this regard.

On the other hand, the private key corresponds to the WEP encryption is unknown to the attacker as well. These two layers of security makes WEP key process completely leak proof. However, both the WEP key and public key (RSA) used to encrypt the IV is already known to the reader/database server against which the supply is checked. As a result, it can be concluded that the proposed method addresses the common loophole of WEP key algorithm and adds less overhead compared to the existing modified WEP key process [9].

In this paper, we outline a hybrid approach to secure transmission using modified WEP and RSA cryptosystem. In theabove section, existing WEP key generation and transmission technique is discussed and finally, we propose the modified technique in the following section to address some of the issues identified in the existing system.

We propose an RSA public key [16] cryptosystem to encrypt the IVs and transmit over the wireless link. According to the public key cryptosystem only the corresponding private key can decrypt the cipher text made with the public key and as the private key never gets transmitted, a man in the middle attack may never be able to obtain it unless using cryptanalysis technique. A 128 bit RSA key ensures that no known crypt analysis is fast enough to crack such a public key in due time. Only a known plain text attack can be effective against such an encryption. However, an eavesdropper (an attacker in possession of unauthorised RFID readers) may never get access to the IVS in the form of plain text because they are generated from original data and encrypted using the public key of a corresponding private key. Both keys can be secret to the manufacturer making the process completely full proof. The RSA public key cryptosystem is stated below.

The generation of the public and private key pairs takes place according to the following equations.

$$p, q$$
$$n = pq \qquad \phi(n) = (p-1)(q-1)$$
$$e, \qquad 1 < e < \phi(n) \qquad \gcd(e, \phi(n)) = 1$$
$$d = e^{-1} \bmod \phi(n)$$

Figure 4. Generation of key pair using RSA system

Application of RSA system to the WEP key works the following way. The above formula displays both the private and public key used in a crypto system. {e,n} is used as a public key and {d, p, q} serves as a private key none of which ever gets transmitted over the link. We propose encryption of transmitted IV, shown at Figure 2 before transmission over the air. This approach preserves the flavor of WEP key process in a modified and secure way. The generation of cipher text from any plain text is shown on Figure 5.

$$C = M^e \bmod n$$

Figure 5. Cipher text generation process using RSA crypto system

The receiver on the other end possesses the private key and so use the process in Figure 6 to decrypt the IVs.

$$M = C^d \bmod n$$

Figure 6. Decryption technique using RSA crypto system

Figure 7 shows a stereo type block cipher process in which a complete block of plain text is being broken into more than one block and encrypted one by one.

$$C^d \bmod n \qquad n = pq$$
$$C^d \bmod p = C_p$$
$$C^d \bmod q = C_q$$
$$C^d \bmod n \equiv \left(C_p\left(q * (q^{-1} \bmod p)\right) + C_q\left(p * (p^{-1} \bmod q)\right)\right) \bmod n$$

Figure 7. Generating cipher text taking one block at a time

Thus, a chunk of IVs can be encrypted using RSA, sent over the open air link safe and sound and decrypted at the receiving end. The figures given below describe how the hybrid encryption uses a public and private key to secure the plain text transmission of the IVs via open air.

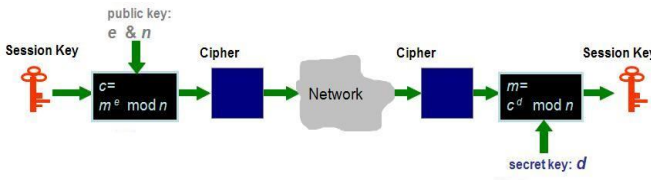

Figure 8.Generation of Session key

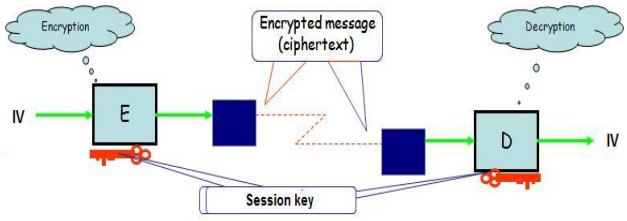

Figure 9.Secure transaction of IVs

6. PROBLEM TO THE HYBRID TECHNIQUE AND A PROPOSED SOLUTION

The process described in the above sub-section, 5.3, uses the following steps to secure the delivery of Initialisation Vector (IV).

- Primarily an asymmetric key algorithm is used for exchanging a symmetric key.
- Once the symmetric key is set up a private encryption algorithm takes over the process using the key and exchange IVs.

In case of a warehouse, countless trucks move in and out throughout the day. Use of a single symmetric key for all trucks maysubject to statistical model base attack to break into the RFID data exchange system. A time frame based approach could be suitable here whichiscapable of resetting the symmetric key after a certain amount of time. However, that may inflict two different problems as discussed below.

- If the session reset takes place in the middle of a scanning session it could slow down the process.
- In case there is no truck waiting at the entrance the system will keep on resetting the key. That may provide enough data to an intruder within a small period of time to guess the reset pattern.

As a result, we propose a laser based scanning system, like one used to check the presence of material over a conveyor belt, placed along the truck entry ramp. Once a truck comes through the laser detector,the system will reset the key and start scanning. As the truck leaves,the session will expire and the RFID scanning stops transmission. Thus, the resources and chances of exposure to a hacker could be minimized. The following Figure 10 portrays the generation and expiry of the proposed session key.

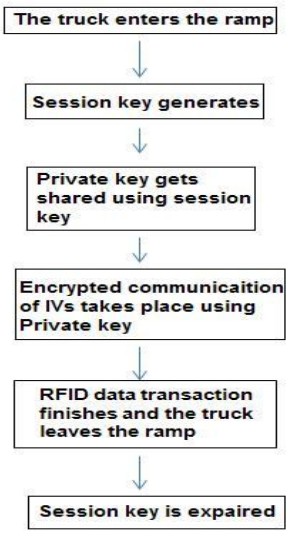

Figure 10. Generation and expiry of the proposed session key

7. CONCLUSIONS AND FUTURE WORK

A RFID-based SCM systems uniquely identify every product in real-time across the supply chain to increase efficiency in areas like retailers, hospitals, farmers, and public transport. The advantages of having RFID system is that its tag's read rate is much faster than the barcode system. However, the data transmission procedure is not secure so far as the wireless mode of transmission can be scanned by another reader in range and so the secrecy of the data is being compromised. Conventional encryption system such as WEP/WPA key encryption can be intercepted and broken using modern techniques. The short fall of WEP key is addressed in this paper. Usually WEP key uses a private key encryption technique which is easy to implement on the available wireless tag reader. The information hiding algorithm works in a straight way. Generation of IV takes place from the data itself and so these vectors are transmitted over the wireless link. A clear text transmission of the IV makes the WEP key process vulnerable to statistical attack. If a person gathers enough amounts of IVs and encrypted text then a comparative process may reveal the secret WEP key used to encrypt the data. A modified approach suggests not to transmit the IV and to use the network traffic control data on both transmitter and receiver end instead. However, the same approach can be used by the attacker as well to determine a group of IVs because WEP key repeats a group of vectors for the encryption process. The proposed system uses a conventional generation of key from the data itself and to transmit the vector with the cipher text. However, unlike the original WEP key algorithm the IVs will be encrypted with a public key created using RSA algorithm. The use of the corresponding private key is the only way to decrypt the cipher text in this case. This private key need not required transmitting over the air and so it stays in the receiving end only.In addition, the session key generation and expiry based on entrance and exit of the trucks makes it more critical to break into a particular session and achieve the session key because of the small life time of one session.

A person performing man in the middle attack may intercept the transmission and keep a copy of the frames travel through the wireless media. The unavailability of the private key still renders the attack impossible to determine the IVs and so the proposal makes the WEP key algorithm leak proof. A brute force attack (gain unauthorized access to a RFID system) on the RSA crypto system may takes several hundred years to find the private key. The use of RFID tag on a supply chain management system speeds up the complete process. As a result, real time key determination using cryptanalysis is impossible in the given scenario.

The ECC approach [25] needs all the hardware to be replaced by the newly build chip which incur considerable amount of cost whereas the proposed approach of this paper requires an additional resource of firmware up gradation while keeping the old system intact.

Finally, the development and implementation of the proposed system could be an interesting area of future research.

REFERENCES

[1] Weis, A. S., Security and Privacy in Radio-Frequency Identification Devices, Master Thesis. MIT,
[2] Glover, B. and Bhatt, H. (2006), "RFID Essentials", O'Reilly Media, Inc. 1005 Gravenstein Highway North, Sebastopol, CA 95472, Jan. 2006, pp. 54-169.
[3] Landt, J. (2005), "The history of RFID," Potentials, IEEE, Vol. 24, No. 4. (2005), pp. 8-11.
[4] Chowdhury, B., Khosla, R and Chowdhury, M. (2008), Real-time Secured RFID-based Smart Healthcare Management System, International Journal of Computer & Information Science (IJCIS), USA, Volume 9, Number 3, 2008 issue.
[5] Banks, J., Hanny D., Pachano, M. A., and Thompson L. G.(2007), RFID Applied, John Wiley &Sonsm, Inc.,Hoboken, New Jersey, p311-318.
[6] B. Glover and H. Bhatt, "RFID Essentials", O'Reilly Media, Inc. 1005 Gravenstein Highway North, Sebastopol,CA 95472, Jan. 2006, pp. 54-169.
[7] Michael, K, &McCathie, L, The pros and cons of RFID in supply chain management, Proceedings of the International Conference on Mobile Business (ICMB'05) , 11-13 July 2005, ISBN - 0-7695-2367-6/05, pp. 623-629.
[8] Beth Bacheldor, Strong sales growth expected for RFID tags, Manufacturers' Monthly, 10 Dec 2007, http://www.manmonthly.com.au/articles/Strong-salesgrowth-expected-for-RFID-tags_z138655.htm accessed on 11 February 2011.
[9] Alarcon-Aquino, V.; Dominguez-Jimenez, M.; Ohms, C. (2008), DESIGN AND IMPLEMENTATION OF A SECURITY LAYER FOR RFID SYSTEMS, Journal of Applied Research and Technology, Vol. 6, Núm. 2, agosto-sin mes, 2008, pp.69-83.
[10] Garfinkel, S., A. Juels and R. Pappu., RFID Privacy: An Overview of Problems and Proposed Solutions, IEEE Security & Privacy. May/June 2005, pp. 34-43.
[11] Stong-Michas, Jennifer, (2006), RFID and supply chain management: this amazing chip will change the world,Alaska Business Monthly: March, 2006 issue.
[12] Nikam, Manish and Satpute, Sagar, (2004) RFID: Changing the face of Supply Chain Management, Welingkar Institute of management development and research, Mumbai, India.
[13] Rao, Sathyajit,(2004), Supply Chain Management: Strengthening the Weakest Link!, Team Leader for Industrial Automation, 1 Mar 2004. http://hosteddocs.ittoolbox.com/SR032604.pdf accessed on 01June 2007.
[14] Michael, K, &McCathie, L, The pros and cons of RFID in supply chain management, Proceedings of the International Conference on Mobile Business (ICMB'05) , 11-13 July 2005, ISBN - 0-7695-2367-6/05, pp. 623-629.Copyright IEEE 2005.
[15] S. Garfinkel and B. Rosenberg, "RFID Applications, Security, and Privacy", Addison-Wesley, New York, USA,2006.
[16] Ronald L. Rivest, Adi Shamir, Leonard M. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. ACM 21(2):pp 120-126, 1978.
[17] Hassan, H. R., and Challal, Y., Enhanced WEP: An Efficient Solution to WEP Threats, IEEE 2nd IFIP International Conference on Wireless and Optical Communications Networks, WOCN 2005, March 2005, pp. 594-599

[18] Purandare, D. S., Enhancing Message Privacy in WEP, Master Thesis, Department of ComputerScience, University of Central Florida, USA, 2005
[19] Fisher, M.L. and Simchi-Levi, D. (2001) Supply Chain Management, www.elecchina.com/ en/doc/osy.htm, accessed 31 May, 2006.
[20] Ambe, I. M. and Badenhorst-Weiss, J. A. (2011) Framework for choosing supply chain strategies, African Journal of Business Management Vol. 5(35), pp. 13388-13397.
[21] Srivastava, B. (2010), Critical Management Issues for Implementing RFID in Supply Chain Management, International Journal of Manufacturing Technology and Management, Volume 21, No. ¾, DOI: 10.1504/IJMTM.2010.035437.
[22] Chowdhury, B and D'Souza, C. (2009), Challenges and Opportunities Relating to RFID Implementation in the Healthcare System, Lecture Notes in Business Information Processing, 2009, Volume 20, Part 2, Part 8, 420-431,Springer Verlag, Heidelberg.
[23] Lo S, Power D (2010). An Empirical Investigation of the relationship between product nature and supply chain strategy. Supply Chain Manage., 15(2): 139-153.
[24] Mukherjee S, Chowdhury B, Hasan M, Chowdhury M. Security of RFID system: A Hybrid Approach, Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2011 12th ACIS International Conference on
[25] Jaspreet Singh, Er. Sandeep Singh Kang. Security Enhancement in WEP by ImplementingElliptic Curve Cryptography Technique, International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-5, November 2012
[26] Laxmi M., Hepzybah.S and Ramadevi.P (2012). Remodelling RC4 Algorithm for Secure Communication for WEP/WLAN Protocol. Global Journal of researches in engineering, Electrical and electronics engineering, Volume 12 Issue 5 Version 1.0 April 2012. Global Journals Inc. ISSN: 0975-586
[27] E. Maxwell. Rethinking privacy. [Online] URL http://www.rdjournal.com/article/view/2133/1/341, last accessed 25/12/2007.
[28] J. Landt. Shrouds of Time: The History of RFID. AIM Publications, Pittsburgh, PA, 2001.
[29] U.W. Thonemann. Improving supply-chain performance by sharing advance demand information. European Journal of Operational Research, 142:81107, 2002.
[30] R. Ranjan, RFID Technology for Supply Chain Management, February 19, 2013, http://cmuscm.blogspot.com.au/2013/02/radio-frequency-identification-rfid-is.html, accessed on 27 May 2013.

AUTHORS

Belal Chowdhury has a multi-disciplinary background in computer science, information system, and management. At present, he is an Academic Course Coordinator (Federation University – IT Programs) at Melbourne Institute of Technology, Melbourne, Australia. Belal has obtained a Master of Computer Science degree from Victoria University, Melbourne in 1998 and Doctor of Philosophy (PhD) in Australian healthcare area at La Trobe University, Melbourne in 2011.
His research focus is Business Intelligence, Data Analytics, and Security in Healthcare Management Systems using emerging technologies (e.g., RFID and sensor). Before joining academia, Belal worked as a Software Engineer/Developer for number of years in different IT disciplines with several multinationals (e.g., IBM GSA,Westinghouse Signal, Mitek Australia, and so on) in the Engineering sector. He has extensive academic and professional/industry experience, and his work has published in internationally refereed journals, book chapters and conference papers. Belal has chaired a conference and reviewed many reputed international journals.

Subhasis Mukherjee has multiple research background in Mathematical security based on Cryptography, Artificial Intelligence and Control System.Currently, he is working as a sessional Lecturer inMelbourne Institute of technology, Australia. Subhasis has obtained a Master degree in Computer Scienceby Research from University of Ballarat, Australia in 2010 and Advanced Diploma in Computer Science from Victoria University Melbourne, 2010 and Bachelor of Electronics and Telecommunication Engineering degree from Vidyasagar University, India in 2003. His research is concentratedon Mathematical Security (Currently being realized on RFID and other wireless based systems) Artificial Intelligence (Applied over Robot)and Control system (Behaviour of various algorithm to control practical sensors). Before joining academia, Subhasis worked as a Communication Engineerfor few years in different IT disciplines with several multinationals (e.g., Hughes Network systems, Reliance Communication, and so on) in the telecommunication sector. He has immense experience in satellite based wireless system, fibre based and PSTN telecommunication system.Subhasis has published 4conference papers and attendedfew international conferences in Australia.

Nasreen Sultana has a multidisciplinary background in Australian health care. At present, she is working as a Senior Emergency Registrar at Monash Health (Dandenong Hospital) in Dandenong, Australia.Nasreen has obtained a MBBS degree from Dhaka University, Bangladesh in 1995 and registration as a medical practitioner from Medical Board of Australia in 2002. Her research interests include Sensor technologies in health care sector. Before joining Monash Health, Nasreen worked as a Medical Practitioner/Registrar for many years in various disciplines (such as medical, surgical, orthopaedics,gynae, plastic and psychiatry) with Frankston and Wangaratta District Base Hospital in Australia.

Maynul Hasan has a multi-dimensional background in Marketing, Management, Accounting, Hospitality Management and Information System. Currently, he is working in Hospitality industry in Keilor East RSL, Melbourne, Australia. Maynul has obtained a

Master of Business Administration degree from University of Ballarat, Australia in 2010 and Bachelor of Science in Business Administration degree from Adamson University, Philippines in 2007.

His research is focused aroundSupply Chain Management facilitated by RFID and other wireless sensors and tendencies of consumer behaviour. Maynul has published 1conference paper. He has attendednumber of international conferences both in Philippines and in Australia.