A Framework For Detecting Bluetooth Mobile Worms

Usman Sarwar, Sureswaran Ramadass and Rahmat Budiarto, *Universiti Sains Malaysia*

Abstract — Bluetooth is an industrial standard for wireless specification for wireless personal area network (PAN). In recent years, Bluetooth technology has become a standard in mobile devices such as cell phones, smart phones and personal digital assistant (PDA) for short range communication. There is a new era of worm attack on these mobile devices through Bluetooth. Few years back worms on cell phones and mobile devices were more like science fiction but these days it is more than a reality. In this paper, our main concern is to detect and prevent malicious propagated code over the Bluetooth network to reduce the chances of epidemic. We propose a framework for detecting Bluetooth worms on public locations such as airports and sports arenas.

***Index Terms*— Worms, Bluetooth worms, Bluetooth worm detection system, Cabir**

I. INTRODUCTION

A worm is a self replicating program which does not need to be part of other programs to propagate and is designed to exploit the vulnerabilities of the computers and policy flaws. In addition to replicating itself, worms may be designed to do various tasks such as deleting files on the host system, send documents or itself for spreading by emails and more recently worms have multi-headed and carry other executables as their payloads. Worms can slow down the network traffic because of its reproduction.

A Bluetooth is radio frequency (RF) technology utilizing the unlicensed 2.4 Ghz industrial, scientific and medical (ISM) band. Bluetooth uses short range radio links, intended to replace the cables connecting portable and/or fixed electronic devices [2]. Its key features are robustness, low complexity, low power and low cost. It is designed to work in noisy frequency environments and it has fast acknowledgement and frequency hopping schemes to make a link robust. There are various applications for Bluetooth which includes PC and peripheral networking, hidden computing and data synchronization such as for address book, synchronization.

Recently mobile devices like cell phones and PDA are the new targeted platform for worms; using Bluetooth and multimedia messaging service (MMS) as their medium of propagation and distribution although few years back, worms and viruses for these types of devices seemed more like science fiction now it is a hard fact. People are not aware that viruses and worms do exist on mobile devices and they use multiple ways like Bluetooth and MMS as a medium of proliferation. Mobile users may use Bluetooth for multiple purposes like transferring of data (for example, Pictures) and network gaming; in doing so the worms from the infected device can infect the non-infected device with worms like cabir.

Malicious code or Worms on the mobile device has somehow the same characteristics of the other worms but with the exception of limited processing power and resources of mobile devices and specifically utilize the features and functionality of these devices like MMS. Although with limited resources these malicious codes are still destructive and will be communal sooner or later. Until now these worms show different behavior and give deficit to the device user for instance crashing the phone, high phone bills, stealing personal information etc.

As the evolution from current generation of cell phones to next generation phones with more capabilities is currently undergoing there is a good possibility of getting higher epidemics in the future. A study released by McAfee Avert labs declares "The number of malicious software programs created for mobile devices is expected to reach 726 by the end of 2006, up from an estimated 226 at the end of 2005"[16]. Another survey conducted by Finnish company F-Secure stated in 2005 "Symbian malware is the vast majority in all mobile malware, but in our opinion this is not because Symbian would be any more insecure compared to other mobile platforms. The large number just shows how popular Symbian devices are, and thus they are the most interesting target for malware authors" [5].

II-AN OVERVIEW OF BLUETOOTH WORMS

Worms using mobile devices have the same characteristics of the other network worms but with the limitation of mobile device processing power and utilization of special features. To advocate our proposed framework, we need to discuss prevalent Bluetooth worms hence we talk about two pioneers of worms on mobile devices SymbOS/Cabir and Commwarrier

A. Symbian Cabir worm

Cabir worm signaled the dawn of a new era of malicious code on the limited computation power devices like phones and PDA. Cabir is considered to be the first worm infection on

mobile devices and targeted the Symbian OS. The worm was first discovered by Symantec on 14 June 2004.

"The worm's code is compatible with mobile phones using ARM series processors with Symbian operating system such as Nokia 60 series. Normally the Bluetooth connection is off on these devices but as the users exchange data such as images and some little programs between their devices, and in doing so they open up the Bluetooth communication channel to Cabir-like worms as well" [10].

Figure 1: Infection of Cabir worm

Cabir replicates over bluetooth connections and arrives in phone messaging inbox as caribe.sis file which contains the worm. When the user clicks the caribe.sis and chooses to install the Caribe.sis file the worm activates and starts looking for new devices to infect over Bluetooth. As the infected device finds another Bluetooth device it will start sending infected SIS files to the target device. Cabir worm can infect only Symbian mobile devices that support bluetooth, and are in discoverable mode. Setting your phone into non-discoverable (hidden) Bluetooth mode will protect your phone from Cabir worm. But once the phone is infected it will try to infect other systems even as the user tries to disable bluetooth from system settings. [10].

Cabir worm uses three phases to spread. In the first phase it searches for Bluetooth enabled devices and connects to the first device found, even if it is a printer or mouse. In the second phase it sends the caribe.sis file to the device. And third stage disconnects from the device. The worm will restart the first stage again and repeat all the phases on the same device while it is allowed. Phase one dramatically reduces the battery power of the device but if Bluetooth is disabled, the worm will not turn it on and hence will not be spread.

There are various variants of this worm which may exploit the devices differently.

B. Symbian Commwarrior

Commwarrier is another mobile worm which propagates using Bluetooth and MMS. It was first discovered in March 2005. It shows the capabilities of mass mailing itself by using MMS. It targetes the Symbian Series 60 smart phones and it propagates randomly named .sis files.

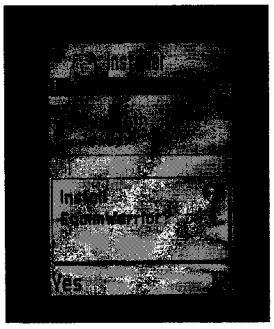

Figure 2. *Arrival of worm by Bluetooth*

Figure 3. *After infection*

The replication approach of this worm is very interesting as it uses different time frames for infection. During the normal user waking hours i.e. 8am to 11:59pm it uses Bluetooth to spread itself as there will be good possibility of other Bluetooth devices within its range. During the normal users sleeping hours which are normally 12:00am to 6:59 am; it uses the phonebook and sends itself by attaching with MMS. It sends MMS after every 10 seconds. The selection of phone number is done by enumerating every contact and looking for mobile numbers which means that land numbers are ignored. The purpose of this procedure is to maximize the propagation of infection to compatible mobile devices. Then from 7:00am to 7:59am it cleans up all the sent MMSes carefully as well as message log afterwards. On the 14th day of every month, worm's payloads activate and reboot the phone in silent mode.

III - RELATED WORK

F-Secure a security company, are the pioneers who did research on mobile-based Bluetooth worms. F-Secure mobile anti virus is a host based worm detection system. Their software application must be installed on the smart phone or PDA to secure the device. As there are different software and hardware platforms available for mobile devices, so they have different versions of applications which ranges from Symbian-based operating system to windows mobile operating system.[13]

Symantec mobile security is another product for symbian series 60 and 80 platforms, including selected models from nokia and Panasonic. This is also a host based detection application. It has a built in firewall for inbound and outbound LAN/WAN communication. It scans for malicious code in SMS, EMS, MMS, HTTP files and email files. [18]

IV- PROBLEM STATEMENT

As we have seen to prevent the device from getting infected it must have host based application software like anti virus which can detect or prevent infection of malware on these mobile devices. Until now most of the work has been done to secure these devices by applications like anti virus software [12] [13] which uses lesser resources because of the limited computation power and capabilities of these devices. They also have the limitation of developed for different platforms.

There is a problem with the current approach, the software must be installed on the device else it will be infected. Moreover the antivirus heuristics must be updated to protect the device.

As technology advances, there will be a possibility of more advanced worms which may create havoc in the usage of mobile devices. Till now, Cabir and Commwarrior worms give us the initial perception of the situation.

If any of the devices does not have the antivirus software, and if it had gotten infected; it will infect many devices within its range. Furthermore there is no means of informing the device owner about the infection. As there is illiteracy among common mobile users about the malicious code, the infection may become severe. Especially when we consider public locations for instance airports, sports arenas, shopping malls. Hence, it can create local and global epidemic as most of the people are not aware of this hazard especially when the device owner travels.

Our proposed system is platform independent as we are developing a Bluetooth network based worm detection system. We will explain the framework in section V.

V. THE PROPOSED FRAMEWORK

We propose a framework for detecting worms on Bluetooth network which we call Bluetooth Network Worm Detection System (BNWDS). It is a defensive system to detect worms or worm attack on the Bluetooth network.

The framework has the following objectives:

1. To detect the worms from the Bluetooth enabled infected mobile devices on PAN level.
2. To stop local epidemic of Bluetooth worms by deploying the system at public locations like sports arenas, hospitals.
3. To stop global epidemic by deploying our framework at airports.

The purpose of the proposed system is to detect worms in Bluetooth networks at public places where there is a good possibility of worms spreading. The system will be flexible enough to be deployed at smaller or larger location.

There are five major entities in our system sensors or sensor nodes, core system, worm heuristics, alarming units and remote heuristics services system as illustrated in figure 4.

The sensors or sensor nodes are used for sniffing Bluetooth packets from piconets or PAN. There can be more than one sensor in our system depending on the required secure coverage area. Each sensor node will cover range depending on Bluetooth power class. Here we are using power class 2 which covers 10 meters or 30 feet range. Class 1 which covers 100 meters can also be used. The sensor nodes will be connected with the core system. All the sensors will have their own unique addresses which will be used by the core system to distinguish the location of the attack. Sensor nodes will sniff the packet and send it to the core system for processing.

The core system is basically an x86 based workstation which has our BNWDS engine running. Sniffed packets are sent by sensor(s) to the core system for analysis and processing. The analysis part will analyze the Bluetooth packet and will authenticate if the packet is from devices like cell phones and PDAs not from devices like printers. After authentication, the packets are moved to detection engines. The core software system consists of a smart engine that utilizes both misuse detection and anomaly detection respectively for better detection and lower false alarm. The sub-core smart engine that handles the matching of the packets data will match the data using a fast algorithm and if any malicious data is detected on the network. An alarm will be activated on the alarming display unit. The second sub-core engine will monitor the ambiguous activities on the network. We state different levels and rules of anomalies into the system. If the ambiguity level found on the network is high; the system will raise an alarm and a message will be sent to the alarming display unit.

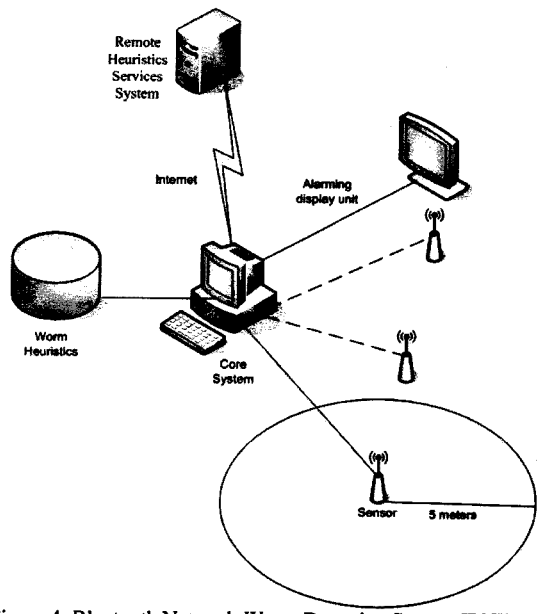

Figure 4: Bluetooth Network Worm Detection System [BNWDS]

The alarming display unit is the vital entity to alert Bluetooth device users about worm propagation in their surrounding area. A message will be displayed and there will be also a vocal announcement to alert users. Alerted display message will advice the Bluetooth device users to turn off their Bluetooth or check their device for worm infection.

Remote heuristics services system use RHS is a web service running on a remote server. RHS will maintain the latest Bluetooth worm signatures in its heuristics. These signatures will be updated by the Bluetooth worm analyst. All core systems will connect with remote heuristics services system periodically through HTTPS to get the latest worm information. RHS will also be responsible to update rules and levels of the BNWDP anomalies engine. Sub-core anomaly engine can also send information about the high ambiguities found on the network to the remote heuristics services. This vital information can provide data to the analysts to investigate those anomalies on the networks.

In short, the proposed system works as follows, whenever a user with an infected device comes within the range of BNWDS sensors, the packets will be captured and sent to the core system for analysis. After the authentication of packet type; the matching sub-core system of the smart engine will analyze the packet and if any malicious data found, it will call the alarm to notify the users. Subsequently, anomaly sub-core will also analyze the network in parallel to detect unknown malicious attacks.

As the objective of our propose framework is to detect the propagation and epidemic of Bluetooth malware from mobile devices. We will discuss two models to deploy our system and effectively stop the Bluetooth worm propagation.

Our framework is designed to stop the epidemic at the public places to control the havoc done by the Bluetooth worms.

Simple Modeling of global propagation as an example

The first solution is to deploy the sensors at the entrances of public areas like entrances and lounges of airports as there is a high probability of worm propagation by infected device. Deploying our system at these locations will allow us to control the epidemic at the global level.

Hence for detection of global epidemic we model it at the airport. At the entrances of airport we arranged sensor S1 and sensor S2 i.e S(S1, S2). Each Sensor has the range of 10 meters. Any passengers with the device D1 or D2 entering into the inspection area of S1 or S2, it will be scrutinized. As passenger with the infected device ID1 will come into the inspection zone of S1. The BNWDS will detect the infectious device and will send the alert. Figure 5 illustrates the simple model. Afterwards the Infected device will be put in a quarantine area where it will be disinfected. If the infection is new and detected by the sub-core anomaly engine; the information will be sent to the RHS.

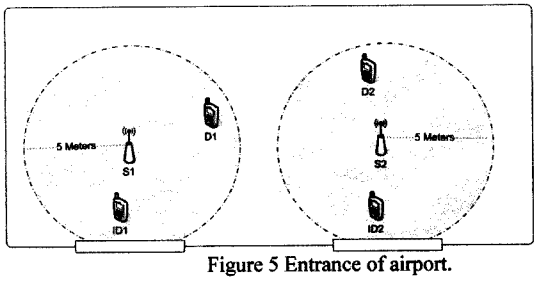

Figure 5 Entrance of airport.

Simple modeling of local epidemic as an example

To control local epidemics, we propose the framework to be deployed at public locations such as sports arenas and shopping malls. The reason behind deploying at these sites is due to detection at early local epidemic and stop at that location.

We did a simple model of detecting worms in sports arenas. We arranged multiple sensors S (S1, S2, ... , S8) in the area. Each Sensor has the range of 10 meters. All the devices D (D1, D2,..., D10) will be within the range of inspection zone. Whenever any infected device ID (ID1, ID2) will be detected; the users will be notified to secure their device which will make the epidemic slower or totally controlled. Figure 6 illustrates the above solution.

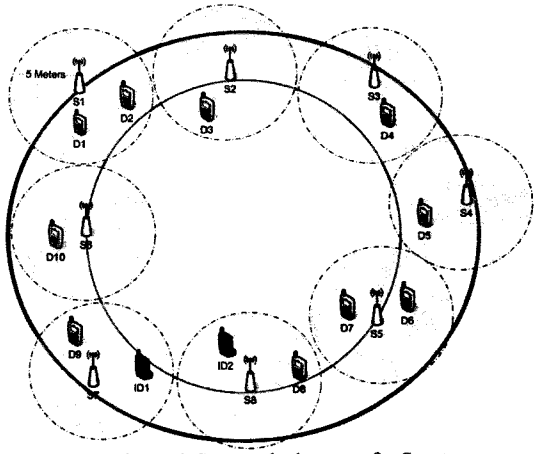

Figure 6, System deployment for Sports arenas.

VI. CONCLUSION

Hence we have presented a framework and also discussed different scenarios where it can detect and solve the worm spreading epidemic. In the future, there will be higher probability of smarter Bluetooth worms; and their propagation and infection. Our Framework will be effective to stop and control the epidemic of Bluetooth worms

VII. FUTURE WORK

In the future, we want to implement the proposed framework and also want to include worm prevention system.

REFERENCES

[1] Zaruba, G.V., Chlamtac, I. Accelerating Bluetooth inquiry for personal area networks.
[2] Specification of Bluetooth system version 1.2, 05 NOVEMBER 2003
[3] Bluetooth 2000: To enable the star generation, Cahners In-Stat group, MM00-09BW, june 2000
[4] S. Krco, "Bluetooth based wireless sensor networks implementation issues and solutions," 10th Telecommunications forum (TELEFOR2002) NOV.2002
[5] Nicholas Weaver (UC Berkeley), Vern Paxson ICSI), Stuart Staniford (Silicon defense), Robert Cunnigham (MIT Lincoln Laboratory). A *taxonomy of computer worms*.
[6] F-secure http://www.f-secure.com
[7] Symantec Corp. http://www.symantec.com
[8] Peter Szor. The Art of Computer Virus Research and Defense. Published by Addison Wesley Professional.
[9] Number of mobile malware close to 100 now by F-Secure http://www.f-secure.com/wireless/news/items/news_2005092800.shtml
[10] F-Secure Virus Descriptions : Cabir. http://www.f-secure.com/v-descs/cabir.shtml
[11] Pravin Bhagwat, Reefedge Inc. Bluetooth: Technology for short range wireless apps.
[12] Symantec anti virus for hand held, http://www.symantec.com/home_homeoffice/products/virus_protection/savhh/index.html
[13] F-Secure Mobile Anti-Virus, http://www.f-secure.com/wireless/
[14] Mobile malware to triple in 2006, http://news.zdnet.co.uk/internet/0,39020369,39242892,00.htm
[15] Virus analysis of Commwarrier by Symantec
[16] Dawn Kawamoto. 2006: Year of the mobile malware. http://news.com.com/2006+Year+of+the+mobile+malware/2100-7349_3-6001651.html
[17] Guanhua Yan and Stephan Eidenbenz. Bluetooth Worms Models, Dynamics, and Defense Implications
[18] Symantec mobile security. http://www.symantec.com/en/ca/small_business/products/overview.jsp?pcid=is&pvid=sms40symb
[19] Jarno Niemela F-secure. F-Secure Virus Descriptions : Cabir. http://www.f-secure.com/v-descs/cabir.shtml
[20] Frederic Perriot, Peter Ferrie and Eric Chien. Symantec security response. Symbian OS Commwarrior,

RFID Technology for Security and Surveillance System.

Muhammad Rafie Hj Mohd Arshad
School of Computer Sciences
Universiti Sains Malaysia
11800 Penang, Malaysia
rafie@cs.usm.my

Abstract

Every year about fifteen millions Muslims visited Makkah to perform Hajj and Umrah. Managing of such a big crowd of people who have come from different parts of the world and are inherited with different types of culture and behaviour is a very challenging task to the authorities. A surveillance system which incorporates RFID technology that could monitor the movement of these pilgrims is needed to help the authorities manage the Hajj and Umrah ritual. The use of RFID will enable head counting and tracking of pilgrim's movement during Hajj and Umrah. Integrating this system with a smart agent will help the decision making process and trigger an alert system in a specific situation. A simplified approach for the implementation of RFID system applications for Hajj and Umrah management is presented. The RFID system architecture will be proposed. The usefulness and merits of the system will be identified and discussed.

Introduction

Every year about two millions Muslims visited Makkah to perform Hajj. Managing of such a big crowd of people who have come from different parts of the world and with different types of culture and behaviour is a very challenging task to the authorities especially in providing them with the best services and ensuring their safety during Hajj. Too many pilgrims with similar objectives packed into a small area may create security threat and safety problems during Hajj. A Hajj monitoring and surveillance system is needed to monitor the crowd, movement of pilgrim; screen and verify the pilgrim's identification, visa information and status of stay. RFID technology which are now being widely used in tracking inventory, cargo, luggage handling and animal tracking will be used in monitoring and surveillance system for Hajj.

RFID Technology

Radio frequency identification, or RFID, is a generic term for technologies that use radio waves to automatically identify people or objects. RFID is one of several technologies collectively known as Auto-ID procedures – procedures for identifying objects automatically. It bridges the gaps to IT systems that were previously bridged by manual data entry. Today, RFID is used in many application including central locking systems for vehicles, toll collection transponders, security and access control, passports, transportation and supply chain tracking etc.

An RFID system typically includes the following components:

- tags
- readers
- radio frequency
- computer applications.

Tags

The RFID tag on an object is mainly a small, wireless microchip with an embedded antenna which will transfer radio waves to a corresponding reader. Various types of tags and labels are available for use in different environmental conditions. The shapes vary from pendants to beads, nails, labels or micro wires and fibres. Tags are generally categorized as either passive or active. "Passive" tags pick up enough energy from the radio to operate and to communicate back to the radio. A passive tag is created with a unique identification number in it. The contents of the chip can never be changed and the ID number is released to a reader when queried. The ID number is then transferred into a computer system containing a database in which the ID is associated with product characteristics. "Active" tags have an embedded battery and offer the advantage of longer-range communications. It may contain a great deal more information and this information can be written, erased, and rewritten from an external read/write device. These chips can contain a history of transactions with read/writers that tracks their progress through a supply chain, medical treatment, or any other process. These chips are considerably more expensive and require security measures to insure that hackers are not able to change the contents of the chip.

Readers

The reader, sometimes called the interrogator, sends and receives radio frequency data to and from the tag via antennas. A reader may have multiple antennas

that are responsible for sending and receiving the radio waves. Tags and readers must have compatible frequencies. Other important factors besides the frequency are the antenna design, range and the transmission power. Readers differ functionally and technically according to their purpose. It comes in different types such as gate readers, compact readers, vehicle-mounted readers, fixed mounted readers and mobile readers. The readers must be highly tolerant as regards to extreme weather conditions and must be protected against dust and damp. It must also support suitable interfaces, for instance:

- WLAN and internet (via Ethernet and TCP/IP),
- point-to-point connection (RS422 or RS232)
- Mobile communication (GSM, GPRS or UMTS) (BITCOM, 2005).

Radio Frequency

RFID uses radio waves to transfer information from a tag where data has been stored to a reader. Just as our radio tunes in to different frequency to hear different channels, RFID tags and readers have to be tuned to the same frequency to communicate. Radio waves behave differently at different frequency, so we have to choose the right frequency for the right application. Four primary frequency bands have been allocated for RFID use:

- **LF (Low Frequency)** (125 – 134 KHz) – has a reading range about 10cm, slow multi tag reading rate, most commonly used for access control, animal tagging, and vehicle immobilizes.
- **HF (High Frequency)** (13.56 MHz) – has a reading range about 1m, medium multi tag reading rate, most commonly used for smartcards, access control, payment, ID, item level tagging, baggage control, biometrics, libraries, laundries, transport & apparel.
- **UHF (Ultra High Frequency)** (860 – 960 MHz) – has a reading range between 2 to 7 m, faster multi tag reading rate, typically used in supply chain pallet and box tagging, baggage handling, electronic toll collection.
- **Microwave** (2.45 GHz – 5.8 GHz) – used for long range access; more than 10m, much faster multi tag reading rate, performance degraded by liquid & metal, commonly being used for electronic toll collection, and real time location of goods. (Paxar, May 2006)

Computer Applications.

Computer applications receive the information from the reader for business services and processes. A middleware is needed in the deployment and use of RFID. Middleware connects readers to the enterprise systems and data repositories. It is also assist in filtering data more effectively and to remotely monitor, control and maintain readers.

How does an RFID system work?

There are several methods of identification, but the most common is to store a serial number that identifies a person or object, and perhaps other information, on a microchip that is attached to an RFID tag. The tag enables the chip to transmit the identification information to a reader. The reader converts the radio waves reflected back from the RFID tag into digital information that can then be passed on to computers that can make use of it. For example, if we want to identify an item:

(i) The reader sends out electromagnetic waves, depending upon its power output and radio frequency.

(ii) When an RFID tag passes through the electromagnetic zone; it detects the reader's activation signal.

(iii) The reader decodes the data in the tag. Compare & match the ID

(iv) The data is passed to the computer for processing or get the information about the item from the computer without having employees type it in.

Advantages of RFID.

Unlike bar code-based tracking systems, an RFID system can read the information on multiple tags without requiring line of sight, without contact and without the need for a particular orientation. That means RFID systems can be largely automated, reducing the need for manual scanning hence reducing data entry errors. In addition, RFID tags hold much more data than UPC labels. The tag can be programmed to hold information such as an item's serial number, personal identification data, as well as a list of all stop points the item pass through before arriving at the destination. Some RFID systems allow companies to write information to the tag and store it there; the RFID tag then essentially acts as a portable, dynamic database. Other systems allow the information contained on the tag to be edited, added to or locked.

RFID for Hajj and Umrah Management.

The adoption of RFID into Hajj and Umrah management is to provide new efficiencies, improved services, and enhanced Hajj and Umrah activities flow. Before implementing RFID project, a strategic Information System Planning (ISP) is needed to produce an overall view of projects across agencies

that may be performing similar functions, generating redundant data, or demonstrating a need for sharing data or resources. This overall view will assists the Arab Saudi authorities in addressing the need for sharing data among agencies in order to facilitate better service to the pilgrims. Projects development will based on the Strategic Plan and resource availability; adherence to the information systems architecture, policies and procedures; and contribution to fulfilment of service delivery to the pilgrims. Figure 1, show a System Architecture for Hajj and Umrah Management RFID applications. This architecture will simplify the process of developing, installing, operating and maintaining the RFID system.

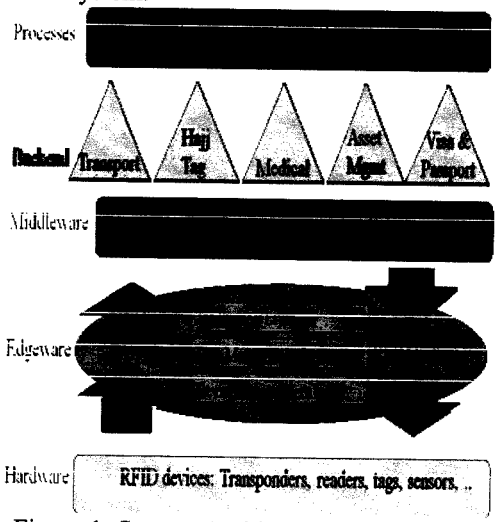

Figure 1: System Architecture for Hajj and Umrah Management RFID Applications

The RFID readers that read the tags are located in the lower hardware layer. The data read is transferred to the edgeware layer which will filter the data so that only the data that is relevant (event or alerts) for the higher layers is transferred to the middleware. The middleware act as a bridge to the application systems in the back end (Bitcom 2005). Some of the application Systems identified for Hajj and Umrah Management RFID applications are:

- **Smart Passport and Umrah Visa Label** – it will store personal information, visual data page of the passport, visa and biometric information. The system is able to record automatically travel history (time, date & place) of entries and exits. Deployment of the system will speed up immigration check in and out resulting in less waiting time. It will also provide a more consistent and reliable method of determining when the pilgrim leave the country.
- **Human Resource Management** - for time and attendance, identification/verification of workers and security personnel, controlled access of personnel to secured locations and activity tracking & monitoring.
- **Asset Tracking & Management** – for tracking the location, movement and maintenance history of physical assets around Masjidil Haram.
- **Medical** - used for patient tracking, storing and access control to patient medical records, drug and medical equipments tracking.
- **Transportation** - used for traffic management, fleet & transport management and tracking, fuel dispensing and maintenance operation, etc.

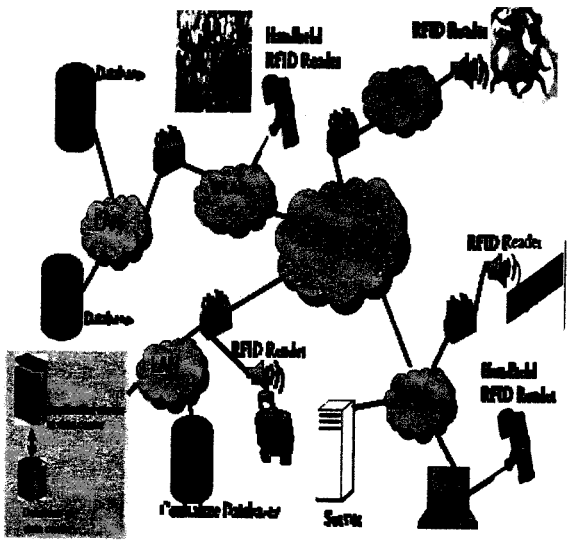

Figure 2: RFID Hajj and Umrah Management Applications and Communication Structure

Hajj Monitoring and Surveillance System

A pilgrims tagging system using hand wrist RFID passive tag will be used in the monitoring and surveillance system for Hajj. The system will consist of an application server, a centralized databases and about two hundred readers (mobile and fixed mounted) which will be deployed around Masjidil Haram as depicted in figure 2. This system will be used for:

- monitoring the human crowd and pilgrims' movement,
- security surveillance by remotely verify the identity and visa status of a pilgrim,

- head count of pilgrims in each location,
- tracking and locating the location of a pilgrim or a lost person,
- analyzing and understanding the behavior of pilgrims in performing hajj activities,
- identify the identity of a person in the event of accident, disaster and tragedy,
- electronic monitoring of offenders

The system consists of four modules:-

1. **Pilgrim Tag Management Module** - major functions in this module are tag registration and tag assignment to a pilgrim.
2. **Central Control/User Management Module** – this module is used to create new user group for management console, create new user account, and update existing user account and user group.
3. **Pilgrim Tracking Module** - the main functions of this module is to do head count, crowd control, monitor and track the movement and location of a pilgrim, analyze the behavior of pilgrims, maintain an alert and activity log system.
4. **Audit Trail Module** – this module is to keep track of each user activities within the system, it provide the records of the user's movement.
5. **Reporting Module** – provides various types of report such as total entry to a selected place, movement of the pilgrims, etc

This system will enable real time data collection, storage, analysis, and distribution. These data can be used for crowd control by doing head counting at a specific location. The density of the crowd could be determined and informed to the pilgrims using electronic billboard or by SMS. Integrating this system with a smart agent will help the decision making process and trigger an alert system in a critical situation. For example, if the crowd is too big, the system will alert the authorities so that they can limit or close the access to the area; hence stampedes tragedy could be avoided. This system can also be used to track the locations of pilgrims who are lost while doing Hajj by identifying the reader they last passed through. The data collected can also be used for pilgrims' behaviour analysis during Hajj with respect to their movement from one place to another; such as where and when they go, duration of the journey and how long they stay at a particular location.

A number of factors influence the suitability of RFID application. Some of it is discussed in the Technical Challenges topic below. The application needs must be carefully determined and examined with respect to the attributes that RFID technologies can offer. Further considerations have to be made in respect of application environment, technical requirements, standards and legislation concerning use of frequencies and power level.

Technical Challenges

On the surface, the technology is very straightforward, but there are a number of very interesting features, limitations, and weaknesses of the systems that many users do not understand. For a detailed discussion of these we recommend (Molnar, 2004) and (Shutzberg, 2004). The most important of these are summarized below (Shutzberg, 2004; Molnar, 2004; Sliwa, 2005, Angeles, 2005):

- **Frequency, Power & Range** - The range of a reader/tag pair is determined by the frequency of transmission and the power transmitted by the reader. The RF spectrum is tightly controlled and heavily used. In the Saudi Arabia, RFID systems will operate in the 860 - 869 MHz and 923 – 960 MHz range.
- **Interference from Materials and RF Devices** - Devices are subject to many sources of interference. Readers typically cannot penetrate metals or liquids. Therefore, products containing these materials must be tagged and handled such that the material does not come between the reader and the tag. Interference also comes from other RF devices like bar code scanners, cordless phones, walkie-talkies, wireless networks, and security systems.
- **Multiple Reads** - The RF wave from a reader triggers transmission in all tags within range. Therefore, a reader must contend with multiple simultaneous signals and multiple transmissions from each tag.
- **Accuracy of Reads** - Wal-Mart's experience is that fully loaded pallets have a read rate of 66%, cases on stocking carts 90%, conveyor belts 95%, and trash compactors 98%.
- **Triangulation** - Identifying the location of a specific tag requires triangulation from multiple readers that are placed in very specific patterns. A large number of readers are required to provide locations in a large area.
- **Speed of reading** - Cases move through a Wal-Mart distribution center at 8 MPH. Readers must correctly identify a product at this pace.
- **Standard protocol, Frequencies, ID Codes** - A number of standards in frequency, power, transmission encoding, data storage, and encryption are needed to make the systems work. Some of these are: ISO/IEC 18000 Part 6,