International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-2, Issue-6, November-2014

The Security of the Transferred Information for Critical Applications in Wireless Communication

Mr.Yannam Apparao, Mrs.K.Laxminarayanamma, Mr. Vijay Katturi

***Abstract*-The development of wireless communication has changed the way of live. : Cellular Telephone Systems, Cordless Phones and Satellite Networks are common place, and many users carry devices that can double as wireless computers, sending text messages, photos and files on the go. Wireless technology has also had an enormous impact in the workplace, improving communication, in this paper developed a security for sending and receiving the text and images in critical application in this paper proposed a frame work for providing the security and also increasing efficiency and introducing new ways of performing many different business tasks.**

***Keywords*-Wi-Fi technology, ICT, WiMAX, local area network, standards, access point**

I. INTRODUCTION

Wireless communication is already common and is still gaining momentum as new uses are constantly being identified. Current uses are as diverse as cellular (smart)phones, Wi-Fi, GPS, security systems, health care, computer interface devices (e.g. Bluetooth), wireless sensor networks and many more. A wireless communication network has numerous advantages, not least the mobility of the devices within the network. It is a simple matter to relocate a communicating device, and no additional cost of rewiring and excessive downtime is associated with such a move. It is also a simple matter to add in a communication device to the network or remove one from the network without any disruption to the remainder of the system. Other than the initial outlay on setting up a wireless network, the cost of running and maintaining it is minimal. These factors show the appeal of wireless technology for the home and office environment. Despite these advantages, one has to take several matters into account before deciding in favor of a wireless alternative over a wired one:

1. The limited spectrum available for wireless communication;
2. The effect of wireless communication on health;
3. The security of the transferred information in critical applications.

II. RELATED WORK

Wireless communications is, by any measure, the fastest growing segment of the communications industry. As such, it has captured the attention of the media and the imagination of the public. Cellular systems have experienced exponential growth over the last decade and there are currently around two billion users worldwide. Indeed, cellular phones have become a critical business tool and part of everyday life in most developed countries, and are rapidly supplanting antiquated wire line systems in many developing countries. In addition, wireless local area networks currently supplement or replace wired networks in many homes, businesses, and campuses. Many new applications, including wireless sensor networks, automated highways and factories, smart homes and appliances, and remote telemedicine, are emerging from research ideas to concrete systems. The explosive growth of wire-less systems coupled with the proliferation of laptop and palmtop computers indicate a bright future for wireless networks, both as stand-alone systems and as part of the larger networking infrastructure. However, many technical challenges remain in designing robust wireless networks that deliver the performance necessary to support emerging applications. In this introductory chapter we will briefly review the history of wireless networks, from the smoke signals of the pre-industrial age to the cellular, satellite, and other wireless networks of today. We then discuss the wireless vision in more detail, including the technical challenges that must be overcome to make this vision a reality. We describe current wireless systems along with emerging systems and standards. The gap between current and emerging systems and the vision for future wireless applications indicates that much work remains to be done to make this vision a reality.

Manuscript received November 25, 2014.
Mr.Yannam Apparao, MLR Institute of Technology & Management Dundigal, Quthbullar(M),R.R.Distic,Hyderbad-500043,Andhra Pradesh, India,Mobile Number:08418-255055/200378
Mrs.K. Laxminarayanamma, Institute of Aeronautical Engineering (Affliated to JNTU, Hyderabad.Approved by AICTE), Dundigal, Qutbullapur Mandal.R.R District.Hyderabad-500043, Andhra Pradesh, India,
Mr. Vijay Katturi, MLR Institute of Technology & Management Dundigal, Quthbullar(M),R.R.Distic,Hyderbad-500043,Andhra Pradesh, India,Mobile Number: 08418-255055/200378

A. Wireless Vision

The vision of wireless communications supporting information exchange between people or devices is the communications frontier of the next few decades, and much of it already exists in some form. This vision will allow multimedia communication from anywhere in the world using a small handheld device or laptop. Wireless networks will connect palmtop, laptop, and desktop computers anywhere within an office building or campus, as well as from the corner cafe. In the home these networks will enable a new class of intelligent electronic devices that can interact with each other and with the Internet in addition to providing connectivity between computers, phones, and security/monitoring systems. Such smart homes can also help the elderly and disabled with assisted living, patient monitoring, and emergency response. Wireless entertainment will permeate the home and any place that people congregate. Video teleconferencing will take place between buildings that are blocks or continents apart, and these conferences can include travelers as well, from the salesperson who missed his plane connection to the CEO off sailing in the Caribbean. Wireless video will enable remote classrooms, remote training facilities, and remote hospitals anywhere in the world. Wireless sensors have an enormous range of both commercial and military applications. Commercial applications include monitoring of fire hazards, hazardous waste sites, stress and strain in buildings and bridges, carbon dioxide movement and the spread of chemicals and gasses at a disaster site.
These wireless sensors self-configure into a network to process and interpret sensor measurements and then convey this information to a centralized control location. Military applications include identification and tracking of enemy targets, detection of chemical and biological attacks, support of unmanned robotic vehicles, and counter-terrorism. Finally, wireless networks enable distributed control systems, with remote devices, sensors, and actuators linked together via wireless communication channels. Such networks enable automated highways, mobile robots, and easily-reconfigurable industrial automation.

B. Cellular Telephone Systems

Cellular telephone systems are extremely popular and lucrative worldwide: these are the systems that ignited the wireless revolution. Cellular systems provide two-way voice and data communication with regional, national, or international coverage. Cellular systems were initially designed for mobile terminals inside vehicles with antennas mounted on the vehicle roof. Today these systems have evolved to support lightweight handheld mobile terminals operating inside and outside buildings at both pedestrian and vehicle speeds

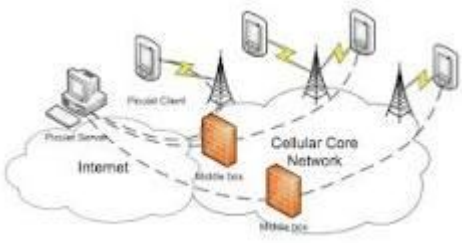

Fig 1: Cellular Telephone Systems

C.Cordless Phones

The base units of cordless phones connect to the PSTN in the exact same manner as a landline phone, and thus they impose no added complexity on the telephone network. The movement of these cordless handsets is extremely limited: a handset must remain within range of its base unit. There is no coordination with other cordless phone systems, so a high density of these systems in a small area, e.g. an apartment building, can result in significant interference between systems. For these reason cordless phones today have multiple voice channels and scan between these channels to find the one with minimal interference. Many cordless phones use spread spectrum techniques to reduce interference from other cordless phone systems and from other systems like baby monitors
And wireless LANs

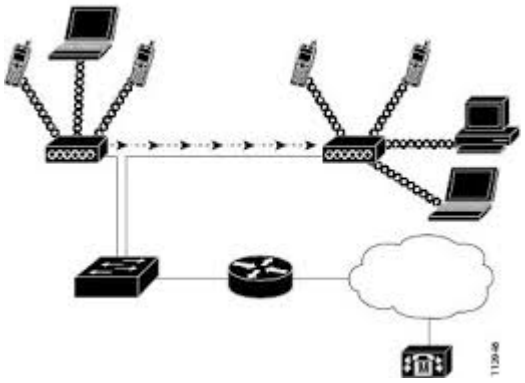

Fig 2: Cordless Phones

D.Satellite Networks

Commercial satellites systems are another major component of the wireless communications infrastructure [6, 7].Geosynchronous systems include Inmost and Omni TRACS. The former is geared mainly for analog voice trans-mission from remote locations. For example, it is commonly used by journalists to provide live reporting from war zones. The first generation In marsat-A system was designed for large (1m parabolic dish antenna) and rather expensive terminals. Newer generations of In marsats use digital techniques to enable smaller, less expensive terminals, around the size of a briefcase. Qualcomm's Omni TRACS provides two-way communications as well as location positioning. The

system is used primarily for alphanumeric messaging and location tracking of trucking fleets. There are several major difficulties in providing voice and data services over geosynchronous satellites. It takes a great deal of power to reach these satellites, so handsets are typically large and bulky. In addition, there is a large round-trip propagation delay: this delay is quite noticeable in two-way voice communication. Geosynchronous satellites also have fairly low data rates, less than 10 Kbps. For these reasons lower orbit LEO satellites were thought to be a better match for voice and data communications.LEO systems require approximately 30-80 satellites to provide global coverage, and plans for deploying such constellations were widespread in the late 1990's. One of the most ambitious of these systems, the Iridium constellation, was launched at that time. However, the cost of these satellites, to build, launch, and maintain is much higher than that of terrestrial base stations. Although these LEO systems can certainly complement terrestrial systems in low-population areas, and are also appealing to travelers desiring just one handset and phone number for global roaming, the growth and diminished cost of cellular prevented many ambitious plans for widespread LEO voice and data systems to materialize. Iridium was eventually forced into bankruptcy and disbanded, and most of the other systems were never launched. An exception to these failures was the Global star LEO system, which currently provides voice and data services over a wide coverage area at data rates under 10 Kbps. Some of the Iridium satellites are still operational as well. The most appealing use for satellite system is broadcasting of video and audio over large geographic regions. In the U.S. approximately 1 in 8 homes have direct broadcast satellite service, and satellite radio is emerging as a popular service as well. Similar audio and video satellite broadcasting services are widespread in Europe. Satellites are best tailored for broadcasting, since they cover a wide area and are not compromised by an initial propagation delay. Moreover, the cost of the system can be amortized over many years and many users, making the service quite competitive with terrestrial entertainment broadcasting systems

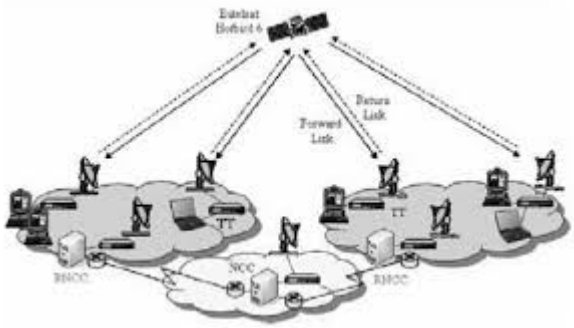

Fig 3. Satellite Networks

III. ADVANTAGES OF WIRELESS COMMUNICATION

I. Using fewer wires means it costs less to set up a network, particularly for large areas of coverage.
II. The more nodes you install, the bigger and faster your wireless network becomes.
III. They rely on the same Wi-Fi standards (802.11a, b and g) already in place for most wireless networks.
IV. They are convenient where Ethernet wall connections are lacking -- for instance, in outdoor concert venues, warehouses or transportation settings.
V. They are useful for Non-Line-of-Sight (NLoS) network configurations where wireless signals are intermittently blocked. For example, in an amusement park a Ferris wheel occasionally blocks the signal from a wireless access point. If there are dozens or hundreds of other nodes around, the mesh network will adjust to find a clear signal.
VI. Mesh networks are "self configuring;" the network automatically incorporates a new node into the existing structure without needing any adjustments by a network administrator.
VII. Mesh networks are "self healing," since the network automatically finds the fastest and most reliable paths to send data, even if nodes are blocked or lose their signal.
VIII. Wireless mesh configurations allow local networks to run faster, because local packets don't have to travel back to a central server.
IX. Wireless mesh nodes are easy to install and uninstall, making the network extremely adaptable and expandable as more or less coverage is needed.

IV. WIRELESS SECURITY ISSUES

There were relatively few dangers when wireless technology was first introduced. Hackers had not yet had time to adapt the new technology and wireless networks were not commonly found in the home and office environment. Today, however, there are a great number of security risks associated with wireless protocols and encryption methods combined with the carelessness and ignorance that exists at the user and corporate IT level. Also, hacking methods have become much more sophisticated and innovative and at the same time much easier and more accessible with easy-to-use Windows or Linux-based tools being made available on the web at no charge.

Some organizations disallow wireless networks and therefore believe they don't need to address wireless security issues. These organizations overlook the fact that wireless security issues can still arise when a wireless laptop is plugged into the corporate network. A hacker could sit out in the parking lot and gather info from it through laptops and/or other devices as handhelds, or even break in through this wireless card-equipped laptop and gain access to the wired network.

Wireless security also compromises location-based services, which are applications that use information

about where a communication device is located. Laws require that mobile telephones are able to provide location data with a fairly detailed accuracy for emergency purposes. Such information also enables location-based services in mobile commerce, which presents a major new market for the telecommunications industry. Unlike other information in cyberspace, location information has the potential to allow an adversary to physically locate a person, and therefore most wireless subscribers have legitimate concerns about their personal safety if such information should fall into the wrong hands.

V. SYSTEM ANALYSIS

The proposed framework is composed of the following three tiers of entities:On the top tier is a dedicated membership server (DMS), which aggregates and periodically disseminates intruder information to the whole network. Due to its critical role, the DMS may become an attractive target of attacks. Specifically, the adversary may locate the DMS and then either compromise the DMS directly or block the communication between the DMS and the rest of the network. To protect the DMS, it is not connected to the network all the time. Instead, it goes online every now and then at different places randomly. The protection makes it hard for the adversary to trace, attack, or isolate the DMS.

On the middle tier are intruder information caches (IICs), which are a small number of sensor nodes picked from all sensor nodes in the network. They temporarily cache new intruder information when the DMS is offline. As ordinary sensor nodes, they could be compromised by the adversary. If compromised, the intruder information cached by these IICs may be removed or modified, which is addressed in our solution through Verifying intruder information to prevent faking or fabricating, Duplicating intruder information to maintain high availability of the information.

On the bottom tier are ordinary sensor nodes, which collaboratively identify intruders and report intruder information to IICs. Sensor nodes maintain their own intruder information based on the periodical updates disseminated by the DMS, and collaboratively determine the legitimacy of sensor nodes that join their neighborhoods; they may also query IICs to obtain latest intruder information when necessary.

To summarize, interactions between these entities include: Sensor nodes collaboratively generate intruder reports that can be verified by any other nodes, and send them to a certain set of IICs. Every time interval l, the DMS queries IICs to collect the reports for intruders that have been identified since the previous query, and then disseminates the IDs of these intruders to all sensor nodes in a secure manner. Upon receiving it, every sensor node records these intruders; if the sensor node is also an IIC, it removes these intruders from its cache. When a node joins a neighborhood, the neighbors can use their own knowledge about identified intruder to determine if the new arrival is intruder or not. If the neighbors need more accurate intruder information, they may query a certain set of IICs to obtain it.

A.Modules Of The Security Of The Transferred Information For Critical Applications

i. Verifiable intruder reporting (VIR) scheme
ii. Collaborative Bloom Filter (CBF) scheme
iii. Quorum based caching (QBC) scheme

Module Description:

i. Verifiable intruder reporting (VIR) scheme:

This scheme which distributed generates the intruder reports that verifiable by any nodes and can prevent malicious nodes from arbitrarily accusing innocent nodes have been compromised Intruder reports generated by a single node are not trustable since the reporting node itself could have been compromised. Therefore, detectors should collaborate to identify intruders, and identification conclusions should be made based on the agreement among the majority of the detectors. After that, intruder information should be known to non-detecting nodes.
A verifiable intruder reporting (VIR) scheme works as follows:

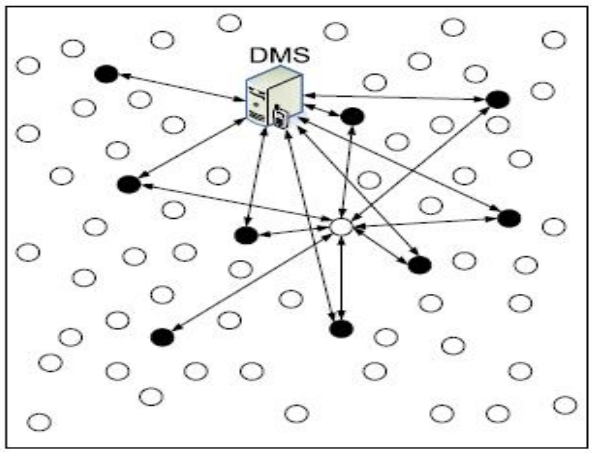

fig 4. Overview of the security of the transferred information for critical applications.

(i) When a node is deployed or relocated to a place, it authenticates with every 1-hop neighbor and disseminates shares of its private key to these neighbors.

(ii) Later, if this node is identified as an intruder by the majority of its 1-hop neighbors, these neighbors can collaboratively derive the private key, which can be used as the intruder report.

(iii) Intruder reports can be verified by every node based on a small amount of secrets preloaded to these nodes.
In this way, verification of intruder reports is easy and decentralized (no need for online trusted membership managers),and the cost for transferring reports is low.

ii. A collaborative Bloom Filter (CBF) scheme:

This module, which consumes only small storage space at each node and meanwhile leverages localized collaboration to enable accurate identification of intruders. The DMS periodically disseminates reports of intruders identified since the last dissemination, and this information should be recorded by each sensor node. As the number of intruders increases and recording these intruders may consume a large portion of sensor nodes' storage, to address this issue, a collaborative Bloom Filter is proposed. To test the legitimacy of a newly deployed or relocated node v, the testing node first searches its own Bloom Filter for v. If v is not found, it is immediately considered as good. Otherwise, neighbors of the testing node are invited to collaboratively test v. Specifically, the testing node broadcasts a query message to its neighbors, each neighbor searches its own Bloom Filter for v, and sends back the result to the testing node. Having received all replies from neighbors, the testing node counts the number of neighbors claiming v as good. If and only if the number is greater than a certain threshold (denoted as γ), v is considered as good.
To test the legitimacy of a newly deployed or relocated node v,

(i)The testing node first searches its own Bloom Filter for v.

(ii)If v is not found, it is immediately considered as good.

(iii)Otherwise, neighbors of the testing node are invited to collaboratively test v.

(iv) The testing node broadcasts a query message to its neighbors, each neighbor searches its own Bloom Filter for v, and sends back the result to the testing node.

(v)Having received all replies from neighbors, the testing node counts the number of neighbors claiming v as good. If and only if the number is greater than a certain threshold (denoted as γ), v is considered as good.

2) False Positive Probability and False Negative Probability:

We use the following notations:
• p: false positive probability when using a single Bloom Filter
• q: probability that a neighbor is innocent (good)
• x: number of neighbors replying "the tested node is good"
• y: number of neighbors replying "the tested node is bad"
• $p(TG)$: probability that the tested node is actually good
• $p(TB)$: probability that the tested node is actially bad
• $p(CG|TB)$ (false negative probability): probability that the tested node is considered good if it is actually bad
• $p(CB|TG)$ (false positive probability): probability that the tested node is considered bad if it is actually good

The response pattern is shown in Table I. For instance, assuming the tested node is good, a good neighbor replies "the tested node is good" with probability $1 - p$, and "the tested node is bad" with probability p; a bad neighbor replies "the tested node is good" with probability p, and "the tested node is bad" with probability $1 - p$. Therefore, it follows that, if the number of replies saying good (x) is greater than threshold γ and thus the tested node is considered good.

TABLE I: RESPONSE PATTERN OF NEIGHBORS

tested node	Good neighbor		bad neighbor	
	reply good	reply bad	reply good	reply bad
good	1-P	p	p	1-p
bad	0	1	1	0

Table .1 Response pattern of neighbors

iii. ***Quorum based caching (Qbc) scheme:***

Quorum based caching (q b c) scheme, which efficiently propagates intruder information through caching intruder information in selected nodes and infrequently updating the information throughout the network;

When a node needs to report an intruder, it randomly chooses *nr* reporting quorums, and then sends an intruder report to the nearest IIC in each of the *nr* reporting quorums via GPSR [20]. These IICs are called *reporting agents*. The communication reliability between the a reporting sensor node and its corresponding *reporting agents* can be achieved using the hand-shake mechanism. After a *reporting agent* receives the intruder report, it propagates the report in two opposite directions to the next IICs in the same reporting quorum, and so on and so forth. Similarly, when a node needs to query for the legitimacy of a new neighbor, it randomly chooses *nq* querying quorums, and then sends a query message to the nearest IIC in each of the *nq* querying quorums. These IICs are called *querying agents*.

The communication between the querying node and its corresponding *querying agents* can also be made reliable. After a *querying agent* receives the query, it checks its list for the queried node. If a match is found, i.e., the queried node has been reported as an intruder, the corresponding intruder report is returned to the querying node. Otherwise, the *querying agent* propagates the query in two opposite directions to the next IICs in the same querying quorum, and so on and so forth. If the querying node receives an intruder query result within a certain *time-out* period (predefined based on the diameter of the network, message propagation speed, and so on), the queried node is considered compromised; otherwise, the node is considered innocent.

VI. PERFORMANCE EVALUATION

To validate our design of the RT-WiFi protocol and evaluate its performance in providing high-speed

real-time wireless communication, we set up a testbed for the performance comparison between RT-WiFi and regular Wi-Fi. As shown in Fig.4, the testbed consists of one AP and three stations (STA1, STA2 and STA3) which form a star network topology. All the four devices are equipped with the same Atheros AR9285 IEEE 802.11 compatible wireless interface but different CPUs with varied computation power.

This is to demonstrate that the implementation of RT-Wi-Fi only introduces limited computation overhead, and can even run on resource-constrained embedded devices. To emulate the sensing and control flows in a wireless control system, we install a UDP socket program on each device. Sensor data with a fixed size payload are transmitted from each station to the AP according to the configured sampling rate on the other direction; the AP periodically transmits control data with the same packet size back to each station. Notice that sensors, actuators, and controllers are all running in the application layer. The overall delay from a sensor to a controller or from a controller to an actuator includes the application layer to MAC layer delay in each device and the MAC layer to MAC layer delay between the devices. In this section we focus on evaluating the MAC layer performance.

We will evaluate the application layer performance in Section VI through a case study. We compare the MAC layer to MAC layer performance between RT-Wi-Fi and regular Wi-Fi in two test scenarios, an interference-free environment and and office environment with Wi-Fi traffic. The main performance metrics we used in the experiments include the data link layer transmission latency and the packet loss ratio. The data link layer transmission latency is calculated as the difference of a frame's TSF timestamps Between the receiver side and the sender side; The packet loss ratio measures the percentage of packets lost by tracking the sequence number of each packet. We shall also consider 145 application-specific performance metrics in our control application in Section

VII. CONCLUSION

Frame work given in this paper provides the security for the transferred information for critical applications in wireless communication, the proposed system is given security for Cellular Telephone Systems, Cordless Phones and Satellite Networks since these are the common has using devise.

REFERENCES

1. [Chandra2005]," BULLETPROOF WIRELESS SECURITY: GSM, UMTS, 802.11, and Ad Hoc Security (Communications Engineering) ,". Newnes 2005

2. [Imai2006]," Wireless Communications Security,". Artech House Publishers 2006

3. [Welch2003] "Wireless security threat taxonomy ,". Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society 18-20 June 2003 Page(s):76 - 83

4. [Edney2003]," Real 802.11 Security: Wi-Fi Protected Access and 802.11i ,". Addison Wesley 2003

5. [Earle2005] "Wireless Security Handbook,". Auerbach Publications 2005

6. [Hardjono2005]," Security In Wireless LANS And MANS ,". Artech House Publishers 2005

7. [Rittinghouse2004]," Wireless Operational Security ,". Digital Press 2004

8. [Prasad2005]," 802.11 WLANs and IP Networking: Security, QoS, and Mobility,". Artech House Publishers 2005

9. [Manley2005] "Wireless security policy development for sensitive organizations," Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005. Proceedings from the Sixth Annual IEEE 15-17 June 2005 Page(s):150 - 157.

10. [Arbaugh2003] " Wireless security is different ,". Computer Volume 36, Issue 8, Aug. 2003 Page(s):99 - 101

Mr. Yannam Apparao, Currently working as Associate Professor, MLR Institute of Technology &Management,Dundigal,Quthbullar(M),R.R.Distic, Telangana-500043.

Mrs. K.Laxminarayanamma,
Currently working as Associate Professor, Institute of Aeronautical Engineering, Quthbullapur(M), R.R.Distic, Telangana, India. Affiliated to Jawaharlal Nehru Technological University,

Mr. Vijay katturi, Currently working as Assistant Professor, MLR Institute of Technology & Management, Dundigal, Quthbullar(M),R.R.Distic, Telangana-500043.