# Critical Review of Security Attacks in Wireless PAN

Dimpal
Student
Department of Computer Science & Application
Maharishi Dayanand University, Rohtak

Priti Gulia
Assit. Professor
Department of Computer Science & Application
Maharishi Dayanand University, Rohtak

## ABSTRACT
Wireless personal area network is a personal area network a network for interconnecting devices centered around an individual person's work space in which the connections are wireless. Typically, a wireless personal area network uses some technology that permits communication within about 10 meters i.e a very short range. One such technology is Bluetooth, which was used as the basis for a new standard, IEEE 802.15. The personal area network computing model allows all network computer system systems to take part within processing but at their respective ends, separately. This model allows sharing data & services but does not help other network computer system systems within processing. After that will study of Existing Security loop holes within wireless PAN based distributed network environment. The security threats are Hacker, cracker, crypto analysts, Brute Force attack , Man in Middle attack, Denial of services. In this research we will make the critical review on security loop holes of existing mechanisms. Then will create a new security mechanism to enhance security of data on wireless personal area network by customizing existing Encryption & Decryption Mechanisms. In this paper a critical review of security attack is discussed.

## Keywords
Wireless, Attack, Decryption, Critical Analysis, Equivalent

## 1. INTRODUCTION
**Wireless Personal Area Network**
Wireless Personal Area Networks (WPANs) is an emerging technology for future short range indoor and outdoor multimedia and data centric applications.

The main objectives of research are to establishment of Distributed Network Environment & creation of Wireless PAN within this Distributed Environment. After that we will study of Existing Security loop holes within wireless PAN based distributed network environment. Then we will create a new security mechanism to enhance security of data on wireless personal area network by customizing existing Encryption & Decryption Mechanisms. The main objective is to boost outer layer security by enhancing packet filter mechanism.

Two types of WPANs have been standardized by the IEEE 802.15 working group; namely: High data Rate WPANs (HR-WPANs) and Low data Rate WPANs (LR-WPANs). These standards define the network architecture, the physical layer and the medium access control sublayer for these systems. A tremendous number of performance studies through mathematical analysis and simulation have been published. Also, many products have appeared in the market which indicate a clear sign of a quick acceptance to the published standards. An organized review of the network architecture, the physical layer specifications, the Medium Access Control (MAC) protocols and the general network operation concepts of the WPAN systems deserves time and effort to be presented in a collective manner. In this paper we describe the concept of WPANs and its applications. Then, the communication architecture and the allocated frequency spectrum for WPAN operation are explained. The developed MAC sublayer protocols in the literature are explored.

Shaping the 4G platform, wireless network solutions are generally focusing on user, and no longer on operators and network providers. The 4G will present an integrated platform that will promote new networking solutions including WPANs (Wireless Personal Area Networks). Development of new paradigm and enhancement of already existing ideas and solutions will hopefully create generic concept of person centred short-range network existing within the personal space surrounding the user. System definition and possible technical solutions are challenging the researchers around the world. This paper gives a closer view on most challenging foreseen topics.

**Architecture**
Currently, two WPAN standards have been developed for advanced short-range wireless communications: IEEE 802.15.3 for High-Rate WPAN (HR-WPAN) and IEEE 802.15.4 for Low-Rate WPAN (LR-WPAN). The HR-WPAN defines the protocols and their primitives for supporting high rate multimedia and data communications over a short-range transmission channel. On the other hand, LR-WPAN standard defines the protocols and their primitives for supporting low data rate communication also over a short-range transmission channels. A WPAN network is featured with low-cost and very low power consumption nodes, ease of installation, reliable data transfer, and simple protocol structure. In addition to the contention- based channel access mechanism, both of the standards adopt the Time Division Multiple Access (TDMA) for assigning one or more exclusive transmission slots to a single node in order to provide Quality of Service (QoS) for the supported applications.

A WPAN consists of several nodes communicate over a wireless channel. One of these nodes is required to assume the role of the network coordinator.2 The network coordinator starts the creation of a WPAN and allocates collision free time slots when requested by network nodes. Also, it controls the association and disassociation process of a node to the network. The WPANs standards are only defined for the physical and medium access control layers and are defined to operate over the Industrial, Scientific and Medical (ISM) frequency bands.

## 2. LITERATURE REVIEW

**Tim Berners-Lee proposed a new project to his employer CERN, with goal of easing exchange of information between scientists by using a hypertext system. The project resulted within Berners-Lee writing two programs within 1990:**

A browser called WorldWideWeb.

The world's first web server, later known as CERN httpd, which ran on NeXTSTEP

Between 1991 & 1994, simplicity & effectiveness of early technologies used to surf & exchange data through World Wide Web helped to port them to many different operating systems & spread their use among scientific organizations & universities, & then to industry. In 1994 Tim Berners-Lee decided to constitute World Wide Web Consortium (W3C) to regulate further development of many technologies involved (HTTP, HTML, etc.) through a standardization process.

**Critical Analysis:**

This research was limited to only web based security

**Wormhole Attacks within Wireless Networks Yih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, & David B. Johnson, Member, IEEE[4]**

As mobile ad hoc network applications are deployed, security emerges as a central requirement. In this paper, we introduce wormhole attack, a severe attack within ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if attacker has not compromised any hosts, & even if all communication provides authenticity & confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location within network, tunnels them (possibly selectively) to another location & retransmits them there into network.

The wormhole attack could form a serious threat within wireless networks, especially against many ad hoc network routing protocols & location-based wireless security systems. For example, most existing ad hoc network routing protocols, without some mechanism to defend against wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication. We present a general mechanism, called packet leashes, for detecting and, thus defending against wormhole attacks, & we present a specific protocol, called TIK, that implements leashes. Topology-based wormhole detection, & show that it is impossible for these approaches to detect some wormhole topologies.

**Critical Analysis :** This research was limited to Wormhole Attacks. Brute force attack problem is not solved here

**IEEE 802.11 Wireless LAN Security Overview was introduced by Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen[1]**

Wireless Local Area Networks (WLANs) are cost effective & desirable gateways to mobile computing. They allow computers to be mobile, cable less & communicate with speeds close to speeds of wired LANs. These features came with expensive price to pay within areas of security of network. This paper identifies & summarizes these security concerns & their solutions. Broadly, security concerns within WLAN world are classified into physical & logical. The paper overviews both physical & logical WLANs security problems followed by a review of main technologies used to overcome them. It addresses logical security attacks like man in the-middle attack & Denial of Service attacks as well as physical security attacks like rouge APs. Wired Equivalent Privacy (WEP) was first logical solution to secure WLANs. However, WEP suffered many problems which were partially solved by IEEE802.1x protocol. Towards perfection within securing WLANs, IEEE802.11i emerged as a new MAC layer standard which permanently fixes most of security problems found within WEP & other temporary WLANs security solutions. This paper reviews all security solutions starting from WEP to IEEE802.11i & discusses strength & weakness of these solutions.

***Critical Analysis:*** This research was limited to addresses logical security attacks like man in the-middle attack & Denial of Service attacks as well as physical security attacks. It does not solves problem of unauthentic decryption

**SECURITY AND PRIVACY IN EMERGING WIRELESS NETWORKS ARTICLE WAS WRITTEN BY DI MA UNIVERSITY OF MICHIGAN-DEARBORN[2]**

Wireless communication is continuing to make inroads into many facets of society & is gradually becoming more & more ubiquitous. While within past wireless communication (as well as mobility) was largely limited to first & last transmission hops, today's wireless networks are starting to offer purely wireless, often mobile, & even opportunistically connected operation. The purpose of this article was to examine security & privacy issues within some new & emerging types of wireless networks, & attempt to identify directions for future research.

**In Lightweight Hidden Services by Andriy Panchenko, Otto Spanioly, Andre Egnersy, & Thomas Engel Computer Science department, RWTH Aachen University, Germany**[5]

Hidden services (HS) are mechanisms designed to provide network services while preserving anonymity for identity of server. Besides protecting identity of server, hidden services help to resist censorship, are resistant against distributed DoS attacks, & allow server functionality even if service provider does not own a public IP address. Currently, only Tor network offers this feature within full functionality. However, HS concept within Tor is complex & provides poor performance. According to recent studies, average contact time for a hidden service is 24s which is far beyond what an average user is willing to wait. In this paper we introduce a novel approach for hidden services that achieves similar functionality as HS within Tor but does so within a simple & lightweight way with goal to improve performance & usability. Additionally, contrary to Tor, within our approach clients are not required to install any specific software for accessing hidden services. This increases usability of our approach. Simplicity makes our approach easier to understand for normal users, eases protocol reviews, & increases chances of having several implementations of protocol available. Moreover, simpler solutions are easier to analyze & they are naturally less prone to implementation failures rather than complex protocols. In this paper, we describe our approach & provide performance as well as anonymity analysis of resulting properties of protocol.

**In PFS: Probabilistic Filter Scheduling Against Distributed Denial-of-Service Attacks[6] Dongwon Seo & Heejo Lee Div. of Computer & Communication Engineering Korea University Seoul,** Korea Distributed denial-of-service (DDoS) attacks continue to pose an

important challenge to current networks. DDoS attacks could cause victim resource consumption & link congestion. A filter-based DDoS defense is considered as an effective approach, since it could defend against both attacks: victim resource consumption & link congestion. However, existing filter-based approaches do not address necessary properties for viable DDoS solutions: how to practically identify attack paths, how to propagate filters to best locations (filter routers), & how to manage many filters to maximize defense effectiveness. We propose a novel mechanism, termed PFS (Probabilistic Filter Scheduling), to efficiently defeat DDoS attacks & to satisfy necessary properties. In PFS, filter routers identify attack paths using probabilistic packet marking, & maintain filters using a scheduling policy to maximize defense effectiveness. Our experiments show that PFS achieves 44% higher effectiveness than other filter-based approaches. Furthermore, we vary PFS parameters within terms of marking probability & deployment ratio, & find that 30% marking probability & 30% deployment rate maximize attack blocking rate of PFS.

**Critical Analysis:** In case of Tim Berners-Lee proposed a new project to his employer CERN, with goal of easing exchange of information between scientists by using a hypertext system. But Critical analysis This research was limited to only web based security.

**In case of Wormhole Attacks within Wireless Networks Yih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, & David B. Johnson, Member But Critical analysis This research was limited to Wormhole Attacks. Brute force attack problem is not solved here**

**In case of In Lightweight Hidden Services by Andriy Panchenko, Otto Spanioly, Andre Egnersy, & Thomas Engel Computer Science department, RWTH Aachen University, Germany. we describe our approach & provide performance as well as anonymity analysis of resulting properties of protocol.**

**In case of In PFS: Probabilistic Filter Scheduling Against Distributed Denial-of-Service Attacks[6] Dongwon Seo & Heejo Lee Div. of Computer & Communication Engineering Korea University Seoul, . In PFS, filter routers identify attack paths using probabilistic packet marking, & maintain filters using a scheduling policy to maximize defense effectiveness.**

**In case of Security And Privacy In Emerging Wireless Networks Article Written By Di Ma University Of Michigan-Dearborn research is that it does not prevent unauthentic decryption of secure data if data is hacked.**

## 3. EXISTING WORK

The major problem is network security against attackers & hackers. Network Security includes two basic securities.

The first is security of data info i.e. to protect data info from unauthorized access & loss.

And second is computer system security i.e. to protect data & to thwart hackers.

Here network security not only means security within a single network rather within any network or network of networks. Now our requirement of network security has broken into two needs. One is requirement of data info safety & other is requirement of computer system security. On internet or any network of an organization, thousands of important data info is exchanged daily. This data info may be misused by attackers.

Data info security is needed for following given reasons:

1. To protect secret data info users on net only. No other person should watcher access it.
2. To protect data info from unwanted editing, accidently or intentionally by unauthorized users.
3. To protect data info from loss & make it to be delivered to its destination properly.
4. To manage for acknowledgement of message received by any node within order to protect from denial by despatcher within specific situations. e.g. let a customer orders to obtaining a few shares XYZ to broader & denies for order after two days as rates go down.
5. To restrict a user to deliver many message to another user with name of a third one. e.g. a user X for his own notice makes a message containing many favorable instructions & sends it to user Y within these a manner which Y accepts message as coming from Z, manager of association.
6. To protect message from undesirable delay within transmission lines/route within order to deliver it to required destination within time, within case of urgency.
7. To protect data from wandering data packets or data info packets within network for infinitely long time & thus increasing congestion within line within case destination machine fails to capture it since of many internal faults.

Application-layer attacks – In this type of attacks are based on cracking applications which run on workstations or server. These types of attacks are common since there are many different applications which run on machines & are susceptible to attacks. Hackers use viruses, Trojans & worms to infect devices & gain important data info.

Exploit attacks – these are usually made by singles who possess strong computing skills & may take advantage of software bugs or misconfigurations. By having enough data info of a specific software, hackers may "exploit" a particular problem & use it to gain access to private data.

In above researches attacks are prohibited. But hackers are becoming more smart as compare to traditional. We need more secure system to prevent unauthentic access.

## 4. PROPOSED WORK

(A) Study of Existing Security loop holes within server

1. Denial of Service & Distributed Denial of Service attacks
2. Brute Force attack
3. Threat from Cryptanalyst
4. Threat from Hacker

(B) Enhancing security by customizing existing Encryption & Decryption MechanismsDevelopment of Basic Encryption & decryption code within Java Socket programming. Enhancing security of cryptography by making key stronger for authentic encryption decryption.

(C) Enhancing outer layer security by enhancing packet filter mechanism

Packet Filter Mechanism would also be enhanced by introducing user defined algorithm to ignore packets from black listed Internet address

Here we have integrated multilayer security. Only person have authentic IP address can decrypt the data.

iptable

| IP | STATUS |
|---|---|
| 1.0.0.1 | 1 |
| 126.0.0.1 | 0 |
| 127.0.0.1 | 0 |
| 128.0.0.1 | 1 |
| * | |

**Fig 1 List of authentic ip Addresses**

One time password would be generated and it would expire after one time use.

dec_code

| DECR_CODE | STATUS |
|---|---|
| ldfjlj2323_2#d | 0 |
| wsdf#$sdf_ | 0 |
| * | |

**Fig 2 List of One time Password for Decryption**

Following figure represents the working of multilayer security in Wireless Personal area network.

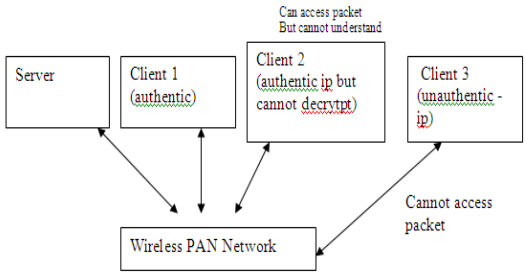


**Fig 3 Proposed Model**

## 5. FUTURE SCOPE

As security mechanism is user defines so further security layer could be added within future. Such security mechanism may be applicable of other server like FTP Server, telnet, SMTP Server. Our security mechanism will first prevent hacker to access data within unauthenticated way & restrict them to understand data. Hacking has both its benefits & risks. Hackers are very diverse. They might bankrupt company or might protect data, increasing revenues for company. Battle btw ethical or white hat hackers & malicious or black hat hackers has been long war, that has no end. While ethical hacker help to understand companies' their security needs, malicious hackers intrudes illegally & harm network for their personal benefits.

## 6. CONCLUSION

In existing system security was limited to web based, man in middle attack or these research were limited to addresses logical security attacks.

Our research restricts access of data from unauthentic IP address. And Data is secured in Encrypted form he can decrypt data only once using one time password after that it would be deactivated. A WPAN consists of several nodes communicate over a wireless channel. One of these nodes is required to assume the role of the network coordinator. The network coordinator starts the creation of a WPAN and allocates collision free time slots when requested by network nodes.

Hackers use viruses, Trojans & worms to infect devices & gain important data info. Ethical & creative hacking has been significant in network security, in order to ensure that company's data has been well protected & secure. At same time this allows company to identify, & in turn, to take remedial measures to rectify loopholes that exists in security system, that might allow malicious hacker to breach their security system. They help organizations to understand present hidden problems in their servers & corporate network. Study also reveals that valid users are ethical hackers, till their intensions are clear otherwise they are great threat, as they have access to every piece of data of organization, as compare to total & semi outsiders. This research has made PAN Difficult to Hack and access to authentic resources has been denied.

## 7. REFERENCES

[1]IEEE 802.11 Wireless PAN Security Overview by Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen, Department of Electrical & Computer Engineering – Sultan Qaboos University, Oman. IJCSNS International Journal of Computer Science & Network Security, VOL.6 No.5B, May 2006

[2] SECURITY AND PRIVACY IN EMERGING WIRELESS NETWORKS BY DI MA UNIVERSITY OF MICHIGAN-DEARBORN, IEEE Wireless Communications October 2010

[3] Efficient Gossip Protocols for Verifying Consistency of Certificate Logs by Laurent Chuat ETH Zurich, Pawel Szalachowski ETH Zurich

[4] Attacks within Wireless Networks Yih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, & David B. Johnson, Member, IEEE, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006

[5] Lightweight Hidden Services by Andriy Panchenko, Otto Spanioly, Andre Egnersy, & Thomas Engel Computer Science department, RWTH Aachen University, Germany within June 2011

[6] In 2011 PFS: Probabilistic Filter Scheduling Against Distributed Denial-of-Service Attacks 36th Annual IEEE Conference on Local Computer Networks, 978-1-61284-927-0/10/$26.00 ©2011 IEEE

[7] D. K. Y. Yau, J. C. S. Lui, F. Liang, & Y. Yam, "Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles," IEEE/ACM Trans. Netw., vol. 13, no. 1, pp. 29–42, 2005.

[8] X. Yang, D. Wetherall, & T. E. Anderson, "TVA: a DoS-limiting network architecture," IEEE/ACM Trans. Netw., vol. 16, no. 6, pp. 1267–1280, 2008.

[9] M. Sung & J. Xu, "IP traceback-based intelligent packet filtering: A novel technique for defending against internet DDoS attacks," IEEE Trans. Parallel Distrib. Syst., vol. 14, no. 9, pp. 861–872, 2003.

[10] S. Savage, D. Wetherall, A. Karlin, & T. Anderson, "Practical Network Support for IP Traceback," within Proc. of ACM SIGCOMM, Aug. 2000, pp.295–396.

[11] K. Park & H. Lee, "On effectiveness of route-based packet filtering for distributed DoS attack prevention within power-law internets," within SIGCOMM, 2001, pp. 15–26.

[12] R. Braga, E. Mota, & A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," within The 35th IEEE Conference on Local Computer Networks (LCN), 2010.

[13] D. Dean, M. K. Franklin, & A. Stubblefield, "An algebraic approach to IP traceback," ACM Trans. Inf. Syst. Secur., vol. 5, no. 2, pp. 119–137, 2002.

[14] J. Jun, M.L. Sichitiu, "The nominal capacity of wireless networks", in IEEE Wireless Communications, vol 10, 5 pp 8-14. October 2003