Wireless Communication Channels: Associated Vulnerabilities & Possible Solutions

Insha Qadir and Yash Tripathi
Pranveer Singh Institute of Technology, Kanpur

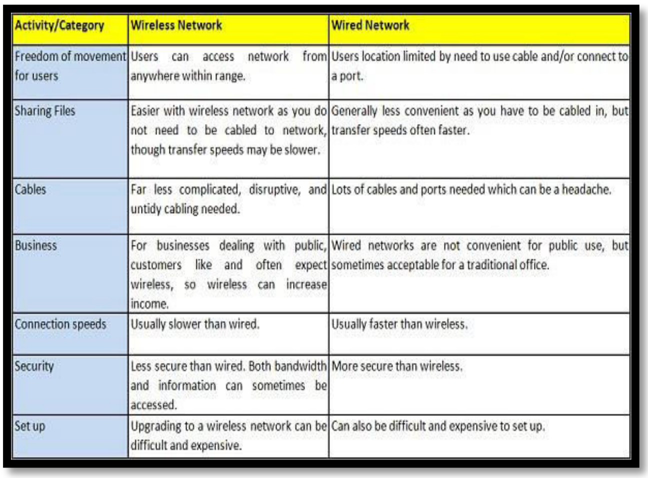
ABSTRACT

In modern communication scenarios, the use of wireless communication channels for data transmission becomes essential. Wireless communication channels are very prone to security attacks. In Denial of Service (DoS) attack, an intruder can intercept the network with targeted messages in order to make sure that the network will not be available for genuine users. Spoofing can be another problem where an intruder pretends to be a legitimate user and performs malicious activities. Eavesdropping is another area of concern where an intruder intercepts the ongoing data by capturing the wireless network. The list of wireless security attacks is even long. So in this context, in this paper, vulnerabilities of wireless communication channels along with the possible solutions are discussed. The up gradation of hardware and software is always a costly and slow process so new security protocols must be developed keeping existing hardware and software infrastructure in mind. The discussion related to security issues and possible solutions of wireless communication channels will be very helpful for the design and development of new concepts and methods.

Keywords**: Wireless Communication, Cryptography, Intruder, Security Issues**

INTRODUCTION:

Wired and wireless communication channels can be compared on many aspects. Wired channels are usually much faster than wireless channels. Wired channels are more reliable and secure comparatively. Wireless channels are better in terms of installation cost and ease of setup establishment. Wired channels suffer with many disadvantages such as lack of mobility, maintenance and cost issues. On the other side, wireless channels are prone to security attacks. The study of communication channels is very important for cryptography and allied areas [1-9], understanding various wireless communication scenarios [10-15] and network security applications [16-20]. A basic comparison between wired and wireless channels is shown in below figure.



Activity/Category	Wireless Network	Wired Network
Freedom of movement for users	Users can access network from anywhere within range.	Users location limited by need to use cable and/or connect to a port.
Sharing Files	Easier with wireless network as you do not need to be cabled to network, though transfer speeds may be slower.	Generally less convenient as you have to be cabled in, but transfer speeds often faster.
Cables	Far less complicated, disruptive, and untidy cabling needed.	Lots of cables and ports needed which can be a headache.
Business	For businesses dealing with public, customers like and often expect wireless, so wireless can increase income.	Wired networks are not convenient for public use, but sometimes acceptable for a traditional office.
Connection speeds	Usually slower than wired.	Usually faster than wireless.
Security	Less secure than wired. Both bandwidth and information can sometimes be accessed.	More secure than wireless.
Set up	Upgrading to a wireless network can be difficult and expensive.	Can also be difficult and expensive to set up.

Fig.1. Showing comparison between wireless and wired channels

The basic security issues of wireless channels are discussed in below points

- ***Denial of Service (DoS) attack:*** Dos attack is used for disabling the services or degrading the performance [21]. DoS attack degrades overall Quality of Service (QoS) of the network. An intruder sends heavy load to the targeted server or device in such a way so that legitimate and genuine users will not be able to access the available resources. Improper configured devices, password vulnerabilities can be the primary cause of DoS attack. The below figure illustrates DoS attack.

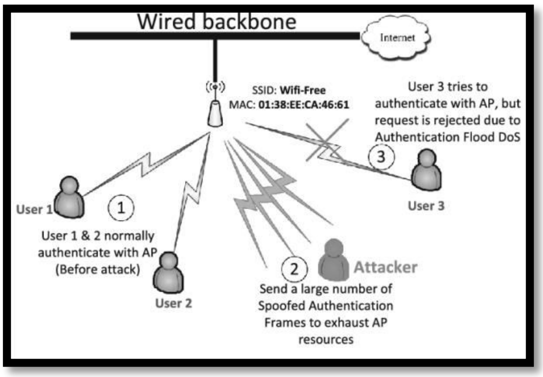

Wired backbone
Internet
SSID: Wifi-Free
MAC: 01:38:EE:CA:46:61
User 3 tries to authenticate with AP, but request is rejected due to Authentication Flood DoS
3
User 3
User 1
1
User 1 & 2 normally authenticate with AP (Before attack)
User 2
2
Attacker
Send a large number of Spoofed Authentication Frames to exhaust AP resources

Fig.2. Showing Dos attack

- ***Eavesdropping***: Eavesdropping attack or snooping attack contains the methods used for obtaining user information [22]. Eavesdropping may include accessing documents in a server or man-in-the-middle attack where an intruder alters the information between two participating entities. Eavesdropping is the result of weak encryption algorithms or keys or loopholes in the communication system. The below figure describes eavesdropping.

ISBN 978-81-931101-3-3 ©2022 Published by Eswar Publications, TN, India

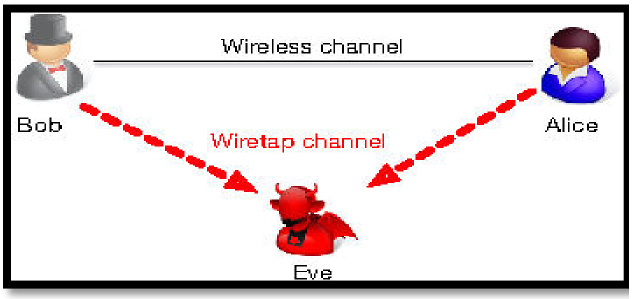


Fig.3. Showing eavesdropping attack where an intruder is in the middle

- ***Signal Jamming***: Signal jamming or wireless jamming can be seen as a specific case of DoS where intruders send malicious signals on a genuine channel by creating intentional interference in the network [23]. An intruder can use of transmitter tuned to the same frequency as the legitimate receiver's equipment with enough power in order to override any signal at the receiver. Random noise, random pulses and tones are used for this purpose. The below figure illustrates signal jamming.

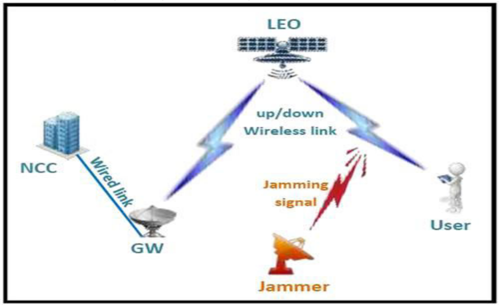
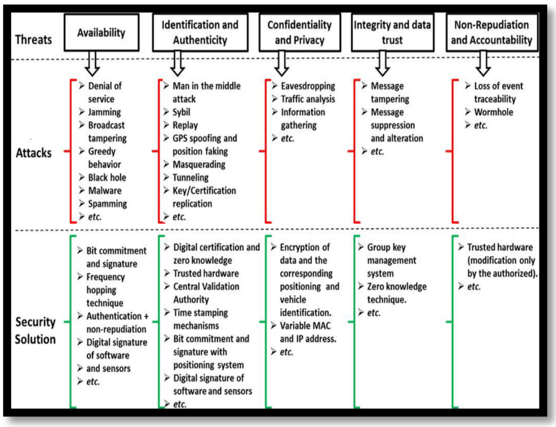


Fig.4. Showing signal jamming

POSSIBLE SOLUTIONS:

These attacks can be prevented if suitable mechanisms are applied. DoS attacks can be prevented by installing firewalls and intruder detection systems as they act as traffic scanners between networks. The session key length also plays a vital role. It should be at least of 256 bits in length. Use of licensed anti virus and anti malware software is very helpful in preventing attacks. Eavesdropping attacks can be prevented by applying strong authentication mechanisms. Two Factor Authentication (TFA) can also be applied as an added layer of security. A Virtual Private Network (VPN) and set of strong passwords with frequent changes are also very helpful in preventing DoS or eavesdropping attacks. Updated hardware and anti jamming techniques are used to prevent signal jamming. The below figure describes the above mentioned problems and solutions in a nutshell.



Threats	Availability	Identification and Authenticity	Confidentiality and Privacy	Integrity and data trust	Non-Repudiation and Accountability
Attacks	➢ Denial of service ➢ Jamming ➢ Broadcast tampering ➢ Greedy behavior ➢ Black hole ➢ Malware ➢ Spamming ➢ *etc.*	➢ Man in the middle attack ➢ Sybil ➢ Replay ➢ GPS spoofing and position faking ➢ Masquerading ➢ Tunneling ➢ Key/Certification replication ➢ *etc.*	➢ Eavesdropping ➢ Traffic analysis ➢ Information gathering ➢ *etc.*	➢ Message tampering ➢ Message suppression and alteration ➢ *etc.*	➢ Loss of event traceability ➢ Wormhole ➢ *etc.*
Security Solution	➢ Bit commitment and signature ➢ Frequency hopping technique ➢ Authentication + non-repudiation ➢ Digital signature of software ➢ and sensors ➢ *etc.*	➢ Digital certification and zero knowledge ➢ Trusted hardware ➢ Central Validation Authority ➢ Time stamping mechanisms ➢ Bit commitment and signature with positioning system ➢ Digital signature of software and sensors ➢ *etc.*	➢ Encryption of data and the corresponding positioning and vehicle identification. ➢ Variable MAC and IP address. ➢ *etc.*	➢ Group key management system ➢ Zero knowledge technique. ➢ *etc.*	➢ Trusted hardware (modification only by the authorized). ➢ *etc.*

Fig.5. Showing possible security threats and security solutions

CONCLUSION & FUTURE SCOPE:

It can be concluded that wireless and wired channels exhibit different characteristics. Wired communication channels are more reliable and fast but having high installation and maintenance cost. Wireless channels are relatively easy to setup but prone to security attacks such as DoS, eavesdropping or signal jamming etc. Use of intrusion detection systems, firewalls or antivirus software is highly recommended along with VPN and strong authentication mechanisms in order to prevent security attacks in wireless channels. Since intruders are gaining new capabilities and high computing power day by day, it is the need of the hour to develop new methods and devices to prevent security attacks. A lot more effort is yet to be done in order to make wireless channels more reliable and secure.

REFERENCES

[1]. V. Shukla, A. Chaturvedi, N. Srivastava, Nanotechnology and cryptographic protocols: issues and possible solutions, Nanomaterials and energy, volume 8, issue 1, 2019, 1-6,
DOI: 10.1680/jnaen.18.00006

[2]. M.K. Misra, A. Chaturvedi, S.P. Tripathi, V. Shukla, A unique key sharing protocol among three users using non-commutative group for electronic health record system, Journal of discrete mathematical sciences and cryptography, volume 22, issue 8, 2019, 1435–1451,
DOI: 10.1080/09720529.2019.1692450

[3]. A. Chaturvedi, N. Srivastava, V. Shukla, A secure wireless communication protocol using Diffie-Hellman key exchange, International journal of computer applications, volume 126, number 5, 2015, 35-38,
DOI: 10.5120/ijca2015906060

[4]. V. Shukla, A. Chaturvedi, M.K. Misra, On authentication schemes using polynomials over non commutative rings, Wireless personal communications, volume 118, issue 1, 2021, 1-9,
DOI: https://doi.org/10.1007/s11277-020-08008-4

[5]. V. Shukla, A. Mishra, S. Agarwal, A new one time password generation method for financial transactions with randomness analysis, Innovations in electrical and electronic engineering (Part of the lecture notes in electrical engineering book series (LNEE, volume 661)), 2020, 713-720,
DOI: https://doi.org/10.1007/978-981-15-4692-1_54

[6]. V. Shukla, A. Mishra, A. Yadav, An authenticated and secure electronic health record system, IEEE international conference on information and communication technology, 2019, 1-5,
DOI: 10.1109/CICT48419.2019.9066168

[7]. A. Chaturvedi, V. Shukla, M.K. Misra, Three party key sharing protocol using polynomial rings, 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2018, 1-5,
DOI: 10.1109/UPCON.2018.8596905

[8]. V. Shukla, A. Chaturvedi, N. Srivastava, Secure wireless communication protocol: to avoid vulnerabilities in shared authentication, Communications on applied electronics, volume 7, number 6, 2017, 4-7,
DOI: 10.5120/cae2017652680

[9]. V. Shukla, M.K. Misra, A. Chaturvedi, Journey of cryptocurrency in India in view of financial budget 2022-23, Cornell university arxiv, 2022, 1-6,
DOI: https://doi.org/10.48550/arXiv.2203.12606

[10]. V. Shukla, N. Srivastava, A. Chaturvedi, A bit commitment signcryption protocol for wireless transport layer security (wtls), IEEE international conference on electrical, computer and electronics engineering , 2016, 83-86,
DOI: 10.1109/UPCON.2016.7894629

[11]. V. Shukla, A. Chaturvedi, N. Srivastava, A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography, Communications on applied electronics, volume 3, number 3, 2015, 16-21,
DOI: 10.5120/cae2015651903

[12]. A. Chaturvedi, N. Srivastava, V. Shukla, S.P. Tripathi, M.K. Misra, A secure zero knowledge authentication protocol for wireless (mobile) ad-hoc networks, International journal of computer applications, volume 128, number 2, 2015, 36-39,
DOI: 10.5120/ijca2015906437

[13]. V. Shukla, A. Chaturvedi, N. Srivastava, Authentication aspects of dynamic routing protocols: associated problem & proposed solution, International journal of recent technology and engineering, volume 8, issue 2, 2019, 412-419,
DOI: 10.35940/ijrte.B1503.078219

[14]. V. Shukla, A. Kushwaha, S.S. Parihar, S. Srivastava, V. P. Singh, Authenticated wireless information display system using GSM module, Communications on applied electronics, volume 5, number 3, 2016, 7-11,
DOI: 10.5120/cae2016652251

[15]. V. Shukla, A. Chaturvedi, N. Srivastava, Double layer cryptographic protocol for mobile ad-hoc networks (MANETs) by commitment scheme, Communications on applied electronics, volume 7, number 9, 2017, 32-36,
DOI: 10.5120/cae2017652716

[16]. V. Shukla, A. Chaturvedi, N. Srivastava, A secure stop and wait communication protocol for disturbed networks, Wireless personal communications, volume 110, 861-872, 2019,
DOI: https://doi.org/10.1007/s11277-019-06760-w

[17]. V. Shukla, A. Mishra, A new sequential coding method for secure data communication, IEEE international conference on computing, power and communication technologies, 2020, 529-533,
DOI: 10.1109/GUCON48875.2020.9231252

[18]. A. Chaturvedi, V. Shukla, M.K. Misra, A random encoding method for secure data communication: an extension of sequential coding, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1189-1204,
DOI: https://doi.org/10.1080/09720529.2021.1932902

[19]. V. Shukla, A. Chaturvedi, N. Srivastava, A new one time password mechanism for client-server applications, Journal of discrete mathematical sciences and cryptography, volume 22, 2019, 1393-1406,
DOI: 10.1080/09720529.2019.1692447

[20]. V. Shukla, M.K. Misra, A. Chaturvedi, A new authentication procedure for client-server applications using HMAC, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1241-1256,
DOI: https://doi.org/10.1080/09720529.2021.1932908

[21]. T. Mahjabin, Y. Xiao, G. Sun, W. Jiang, A survey of distributed denial-of-service attack, prevention, and mitigation techniques, International journal of distributed sensor networks, volume 13, issue 12, 2017, 1-33,
DOI: https://doi.org/10.1177/1550147717741463

[22]. X. Li, H. Wang, H.N. Dai, Y. Wang, Q. Zhao, An analytical study on eavesdropping attacks in wireless nets of things, Mobile information systems, volume 2016, article ID 4313475, 2016, 1-10,
DOI: http://dx.doi.org/10.1155/2016/4313475

[23]. F. Cherifi, M. Omar, T. Chenache, S. Radji, Efficient and lightweight protocol for anti-jamming communications in wireless body area networks, Computers & electrical engineering, volume 98, 2022,
DOI: https://doi.org/10.1016/j.compeleceng.2022.107698