Volume 6, Issue 3, March 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Research Encryption/Decryption in SWiFi Network

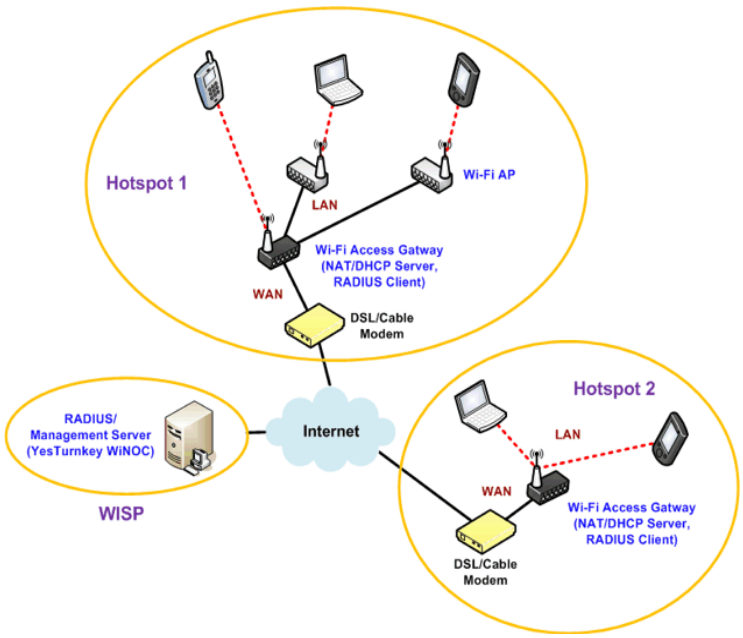
Rashanpreet Kaur, Er. Abhilasha Jain
Giani Jail Singh Campus, Bathinda,
Punjab, India

Abstract—Data integrity and authentication are essential security services in order to secure data transmission process. This research proposed an optimization technique which improves the efficiency of existing secure wifi model.. The proposed technique minimizes the transmission overheads such as delay, network load, retransmission attempts and throughput. This approach reduces these overheads by using Adaptive Ant Colony Optimization (AACO) technique. The proposed system is more efficient than that of existing scheme.

Keywords: WPA, HMAC, PGP, TLS, WEP

I. INTRODUCTION

A computer network or data network is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices exchange data with each other along network links. The connections between nodes are established using either cable media or wireless media. Wi-Fi is a local area wireless computer networking technology that allows electronic devices to network, mainly using the 2.4 gigahertz (12 cm) UHF and 5 gigahertz (6 cm) SHF ISM radio bands. The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network" (WLAN) product based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards".[1] However, the term "Wi-Fi" is used in general English as a synonym for "WLAN" since most modern WLANs are based on these standards. "Wi-Fi" is a trademark of the Wi-Fi Alliance. The "Wi-Fi Certified" trademark can only be used by Wi-Fi products that successfully complete Wi-Fi Alliance interoperability certification testing. Many devices can use Wi-Fi, e.g. personal computers, video-game consoles, smartphones, digital cameras, tablet computers and digital audio players. These can connect to a network resource such as the Internet via a wireless network access point. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometres achieved by using multiple overlapping access points. Depiction of a device sending information wirelessly to another device both connected to the local network, in order to print a document. Wi-Fi can be less secure than wired connections, such as Ethernet, precisely because an intruder does not need a physical connection. Web pages that use TLS are secure, but unencrypted internet access can easily be detected by intruders. Because of this, Wi-Fi has adopted various encryption technologies. The early encryption WEP proved easy to break. Higher quality protocols (WPA, WPA2) were added later. An optional feature added in 2007, called Wi-Fi Protected Setup (WPS), had a serious flaw that allowed an attacker to recover the router's password.[2] The Wi-Fi Alliance has since updated its test plan and certification program to ensure all newly certified devices resist attacks.



II. BACKGROUND

According to (American Bankers, 2000), the Hash Message Authentication code (HMAC) could be a technique that uses cryptographic hash functions for message authentication. This system combines any iterative science with a shared secret key. The HMAC has two parameters, the message and a shared secret key that is thought solely to the sender and receiver. The sender uses HMAC to supply a worth that is represents the mix of the key and therefore the message input, the new price is named raincoat the sender appends the raincoat message and sends all to the receiver. The receiver uses HMAC and a shared secret key, that the sender used before, by applying the raincoat algorithmic rule to the received message and compares the result with the received raincoat. We are able to insure that the message has been correctly received if the 2 values match. There are several steps to use secure WI-FI : initial, the secure WIFI is split into two halves: the primary part is that the plain text for key functions, the second half is split into four pieces; to get and write in code the key mistreatment logical OR-ing and bit shifting of the information during a sure pattern within the four parts. In order to get the key, write code in the primary half and disrupt the probabilistic phenomena of the letters within the language. Finally, at intervals the blocks the encrypted knowledge is shuffled to form cipher text that there is no similarity with original knowledge. (Aljawarneh et al., 2010) Pretty Good Privacy(PGP), is one of the most necessary secret writing and security applications that use economical and confidential algorithms to secure knowledge transmission. The PGP as a secret writing program supported by Phil Zimmerman on 1991 provides complete verification and secret writing for message files (McLaughlin, 2006).

it's supported symmetric-key cryptography and use combination of data compression, hashing and public-key cryptography (Kurniawan, Albone, & Rahyuwibowo, 2011) . (Abdul-Rahman, 1997),(Guibing, Jie, Vassileva, 2011) The PGP is that the initial successful try of a free science model that is accessible for the general public. The sender has the non-public key is able to produce a digital signature for corresponding public key. Digitally, PGP offers alternative users the power to sign certificates that they assume it's authentic, that the owner of the general public secret's an owner of the certificate. To verify a public key, the user has to check if there are any digital signatures that are signed by the trusty users.

PGP compresses the message and creates a public key and a non-public key for the sender through cryptography computer code. Once the plain text is encrypted, the general public secret's encrypted to the receiver's non-public key which might be employed by the receiver to decode the message (Abdul-Rahman, 1997).

Although the PGP is taken into account together of the simplest secret writing techniques, it will have some disadvantages. The PGP could be a two way street that the sender and therefore the recipient should use it, otherwise the recipient won't be able to view the encrypted data(Gibson, 2002).

III. AUTHENTICATION TECHNIQUES

There are two types of authentication services offered by 802.11. The first is Open System Authentication. This means that anyone who attempts to authenticate will receive authentication. The second type is Shared Key

Authentication. In order to become authenticated the users must be in possession of a shared secret. The shared secret is implemented with the use of the Wired Equivalent Privacy (WEP) privacy algorithm. The shared secret is delivered to all stations ahead of time in some secure way.

De-authentication is when either the station wishes to terminate a stations authentication. When this happens the station is automatically disassociated. Privacy is an encryption algorithm, which is used so that other 802.11 users cannot eavesdrop on your LAN traffic. IEEE 802.11 specifies Wired Equivalent Privacy (WEP) as an optional algorithm to satisfy privacy. If WEP is not used then stations are "in the clear" or "in the red", meaning that their traffic is not encrypted. Data transmitted in the clear are called plaintext. Data transmissions, which are encrypted, are called cipher text. All stations start "in the red" until they are authenticated. MSDU delivery ensures that the information in the MAC service data unit is delivered between the medium access control service access points.

The bottom line is this, authentication is basically a network wide password. Wired Equivalent Privacy is used to protect authorized stations from eavesdroppers. WEP is reasonably strong. The algorithm can be broken in time. The relationship between breaking the algorithm is directly related to the length of time that a key is in use. So, WEP allows for changing of the key to prevent brute force attack of the algorithm. WEP can be implemented in hardware or in software.

IV. METHODOLOGY

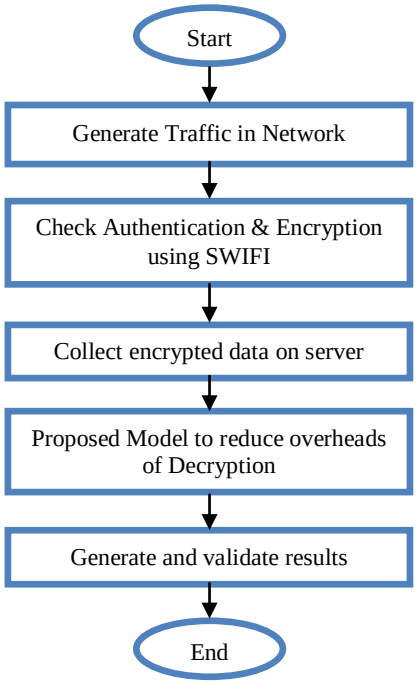
Wi-Fi is a local area wireless computer networking technology that allows electronic devices to connect to the network. Wi-Fi can be less secure than wired connections, such as Ethernet, precisely because an intruder does not need a physical connection. Web pages that use Transport Layer Security (TLS) are secure, but unencrypted internet access can easily be detected by intruders. Because of this, Wi-Fi has adopted various encryption technologies. The early encryption WEP proved easy to break. Higher quality protocols (Wi-fi Protected Access, WPA2) were added later. An optional feature added in 2007, called Wi-Fi Protected Setup (WPS), had a serious flaw that allowed an attacker to recover the router's password. The Wi-Fi Alliance has since updated its test plan and certification program to ensure all newly certified devices resist attacks.

Adaptive Ant Colony Optimization: Adaptive Ant Colony Optimization (AACO) algorithm is a novel meta-heuristic algorithm that has been widely used for different combinational optimization problem and inspired by the foraging behavior of real ant colonies. Adaptive Ant Colony Optimization has strong robustness and easy to combine with other methods in optimization.

In Self-Adaptive Approach, the parameters are encoded into pheromones and undergo mutation and recombination. The idea is that better parameters leads to better pheromones for finding shortest path or largest path, according to combinational problem. In [5], a self-adaptive approach, a single mutation rate is used. With this mutation rate p [0, 1], a new mutation rate p' [0, 1] is found using equation (1). In this equation, γ is the learning rate which controls the adaption speed.

$$p' = \left(1 + \frac{1-p}{p}\exp\left(-\gamma . N(0,1)\right)\right)^{-1} \qquad (1)$$

In this proposed method, Adaptive Ant colony optimization algorithm with uniform mutation operator using self-adaptive approach is used. Here mutation operator is used for enhancing the algorithm escape from local optima. In this method, an additional operator, mutation operator, is used and the new mutation rate is generated by the self-adaptive approach using equation (1). Here AACO algorithm generates the current solution (w). by using mutation operator, random position is changed by new mutation rate in current solution(w). After changing random position, new solution (w') is generated. Then the cost of this new solution (w') is compared by the current solution (w), if the cost of new solution is less than (or greater than) current solution, according to combinational problem, then new solution is replaced by current solution. This process is repeated until maximum iteration is not reached.



FLOW CHART

V. RESULTS

In this research different scenarios are taken into consideration with varying number of nodes against constant simulation time. Comparison is drawn between two encryption algorithms in Privacy-Enhanced Participatory Sensing Infrastructure (PEPSI) architecture on the basis of delay, load, throughput, data dropped and retransmission attempts.

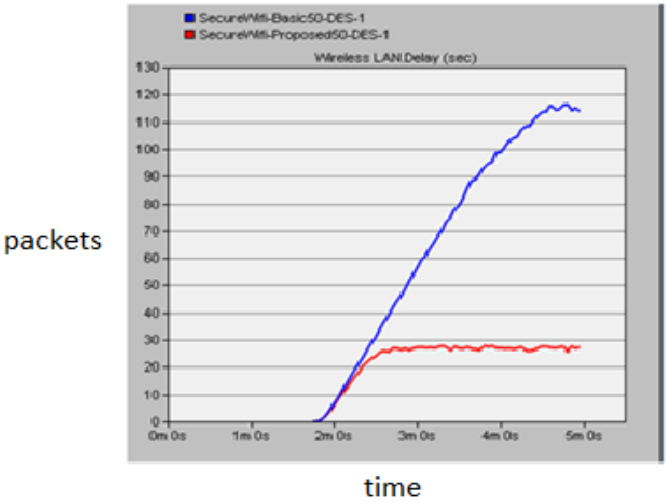


Fig 1: Delay

In the fig 1 a comparative study for delay is presented. In the figure delay for existing scenario is approx 116 sec where as in proposed scenario it is below 30 sec.

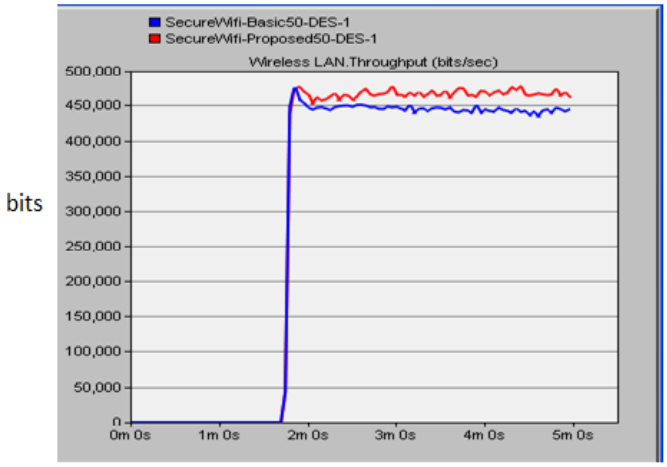


Fig 2: Throughput

In the fig 2 a comparative study for throughput is presented. In the figure throughput for existing scenario is approx. 450,000 bits/sec where as in proposed scenario it is 475,000 bits/sec.

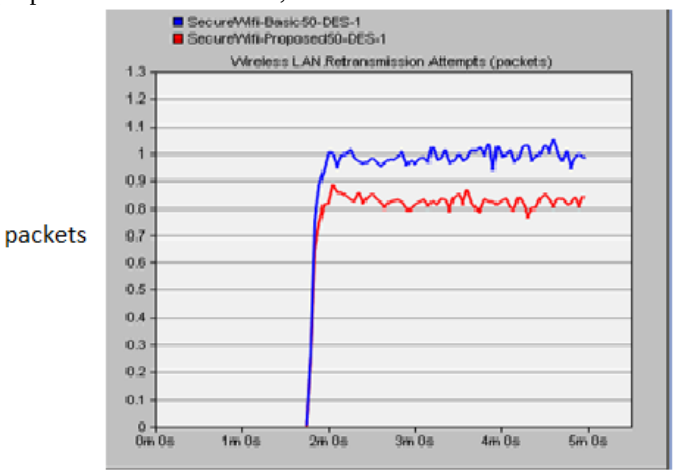


Fig 3: Retransmission Attempts

In the fig 3 a comparative study for retransmission attempts is presented. In the figure retransmission attempts for existing scenario is approx. 1 packet where as in proposed scenario it is below 0.9 packets.

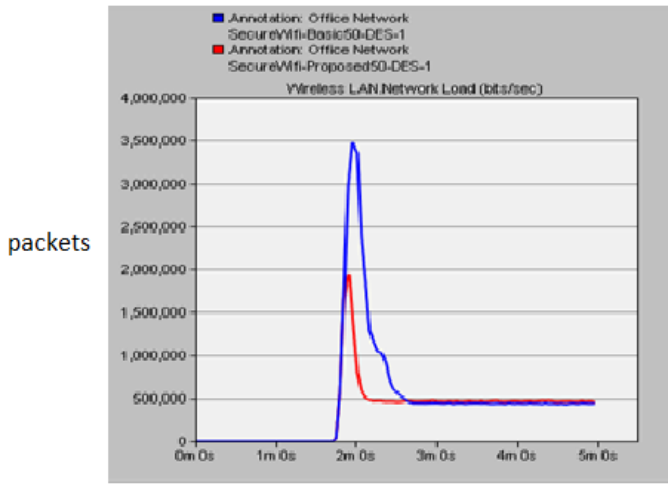


Fig 4: Network Load

In the fig 4 a comparative study for network load is presented. In the figure network load for existing scenario is approx. 3,500,000 bits/sec where as in proposed scenario it is below 2,000,000 bits/sec.

Comparison between Swifi and Swifi with AACO

Parameters	Secure Wifi	Secure wifi with AACO
Delay(sec)	116	30
Media Access Delay(sec)	116	30
Throughput(bits/sec)	450,000	475,000
Retransmission Attempts	1	0.9
Load(bits/sec)	3,500,000	2,000,000

Comparative Study between Swifi and Swifi with AACO

This table represents the comparative study of swifi and swifi with AACO.It shows the effective performance of proposed system in terms of parameters such as delay ,media access delay, throughput ,load etc.

VI. CONCLUSION

Wi-Fi can be less secure than wired connections, such as Ethernet, precisely because an intruder does not need a physical connection. Web pages that use TLS are secure, but unencrypted internet access can easily be detected by intruders. Because of this, Wi-Fi has adopted various encryption technologies. The Internet of nowadays is Janus-faced with several challenges. One in every of the foremost discouraging challenges is to make sure security. Pursuing authentication through applicable mechanisms becomes a posh issue. Among different security problems, authentication and access control are the 2 main fields of security problems that should be resolved to shield info and computing systems against unauthorized access. In this research a scheme is developed using which security is implemented in authorization and authentication process. In spite of implementing the security in the secure Wi-fi the efficiency of the system is not reduces as presented in the results and discussion chapter. From the current study it may be concluded that the proposed system is more efficient than that of existing scheme.

REFERENCES

[1] Abdul-Rahman, A. (1997). The PGP Trust Model. EDI-Forum: The Journal of Electronic Commerce, 10(3), 27-31. doi: citeulike-article-id:8251892

[2] Al-Assam, H., Sellahewa, H., & Jassim, S. (2010). Multi-factor biometrics for authentication: a false sense of security. Paper presented at the Proceedings of the 12th ACM workshop on Multimedia and security, Roma, Italy.

[3] Alaidaros, H. M., Rasid, M. F. A., Othman, M., & Abdullah, R. S. A. (2007, 14-17 May 2007). Enhancing security performance with parallel crypto operations in SSL bulk data transfer phase. Paper presented at the Telecommunications and Malaysia International Conference on Communications, 2007. ICT-MICC 2007. IEEE International Conference on.

[4] Aljawarneh, S., Masadeh, S., & Alkhateeb, F. (2010). A secure wifi system for wireless networks: an experimental evaluation. NETWORK SECURITY(Jun), 6-12.

[5] American Bankers, A. (2000). Keyed hash message authentication code : X9.71-2000. Wash., D.C.: ABA.

[6] Chadwick, D. W., Young, A. J., & Cicovic, N. K. (1997). Merging and extending the PGP and PEM trust models-the ICE-TEL trust model. Network, IEEE, 11(3), 16-24. doi: 10.1109/65.587045

[7] Diffie, W., & Hellman, M. E. (1979). Privacy and authentication : An introduction to Cryptography. Proceedings of the IEEE, 397.

[8] Dusi, M., Gringoli, F., & Salgarelli, L. (2008, 8-10 Sept. 2008). A Model for the Study of Privacy Issues in Secure Shell Connections. Paper presented at the Information Assurance and Security, 2008. ISIAS '08. Fourth International Conference on.

[9] Gibson, D. (2002). Email Security Risks and How To Reduce Them. 1.4.

[10] Griffin, J. A. (1998, 12-13 Jun 1998). Privacy and security in the Digital Age. Paper presented at the Technology and Society, 1998. ISTAS 98. Wiring the World: The Impact of Information Technology on Society., Proceedings of the 1998 International Symposium on.

[11] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," http://www.oecd.org/document/18/0, 3343, en_2649_34255_1815186_1_1_1_1, 00.html.

[12] "IBM Discovers Encryption Scheme That Could Improve Cloud Security, Spam Filtering," at http://www.eweek.com/c/a/Security/IBM- Uncovers-Encryption-Scheme-That-Could-Improve-Cloud-Security-Spam-Filtering- 135413/. Map Reduce," In: Castro M, Eds Proc. of the 7th Usenix Symp. On Networked Systems Design and Implementation. San Jose: USENIX Association, 2010. 297.312.

[13] Roy I, Ramadan HE, Setty STV, Kilzer A, Shmatikov V, Witchel E. "Airavat: Security and privacy for

[14] "OASIS Key Management Interoperability Protocol (KMIP)TC", http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip.

[15] Zeng K, "Publicly verifiable remote data integrity," In: Chen LQ, Ryan MD, Wang GL, eds. LNCS 5308. Birmingham: Springer-Verlag, 2008.419.434.

[16] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing," in Proceedings of the 17th International Workshop on Quality of Service.2009:1-9.

[17] Bowers KD, Juels A, Oprea A. Proofs of retrievability: Theory and implementation. In: Sion R, ed. Proc. of the 2009 ACM Workshop on Cloud Computing Security, CCSW 2009, Co-Located with the 16th ACM Computer and Communications Security Conf., CCS 2009. New York: Association for Computing Machinery, 2009. 43.54. [doi:10.1145/1655008.1655015]

[18] Muntés-Mulero V, Nin J. Privacy and anonymization for very large datasets. In: Chen P , Ed. Proc of the ACM 18th Int'l Conf. On Information and Knowledge Management, CIKM 2009. New York: Association for Computing Machinery, 2009. 2117.2118. [doi:10.1145/1645953.1646333] [19]. Ran dike Gajanayake, Renato Iannella, and Tony Sahama, "Sharing with Care An Information Accountability Perspective," Internet Computing, IEEE, vol. 15, pp. 31-38, July-Aug. 2011.

[19] DOD, "National Industrial Security Program Operating Manual", 5220.22-M, February 28, 2006.

[20] Richard Kissel, Matthew Scholl, Steven Skolochenko, Xing Li, "Guidelines for Media Sanitization," NIST Special Publication 800-88, September 2006, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

[21] Gartner DataQuest Forecast on Public Cloud Services DocID G00200833, June 2, 2010.

