International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.164.04

A Survey on Cryptographic Algorithm for Secure Authentication in Wi-Fi Application

S. Mohamed Iliyas[1], Dr. M. Mohamed Surputheen[2]
[1]*Research Scholar in Computer Science*
[2]*Associate Professor, Department of Computer Science*
Jamal Mohamed College (Autonomous)
(Affiliated to Bharathidasan University)
Tiruchirappalli, Tamil Nadu, India

Abstract- With the advent of the World Wide Web and the emergence of e-commerce applications and social networks, organizations across the world generate a large amount of data daily. Wi-Fi is a very popular Technology. Faster data transfer and Security both are very important for Wi-Fi Supporting mobile applications via public Wi-Fi networks has received significant research attention due to the drastic increase of penetration rate of 802.11-based networks. In this survey explain a various efficient cryptography algorithm which apt to be used on available for Wi-Fi applications.

Keywords:Wi-Fi network, Security, Cryptography, networking process.

I. INTRODUCTION

Wireless network has been an excellent invention at the end of 20th century in inter-network communication. Wi-Fi (wireless fidelity) is one of today's leading wireless technologies (Paul Arana, INFS 612 – Fall 2006) (by George Ou. June 2 2005). Wi-Fi networks based on IEEE 802.11 standard are being widely deployed in different environment due to standardization and ease to use. It allows an Internet connection to be broadcast through radio waves. The waves can be picked up by Wi-Fi a receiver which is attached to computers, personal digital assistants or cell phones. As the businesses expanded wireless demands increased and have become necessity as the day passed.

The networking world suffers from many problems with networks the wireless too are also more prone to problems. Though the problems related to wireless networks is been on constant track to be removed but the solutions are not always perfect. The main two problems that have been faced by the wireless network are security and signal interference. The problem with security can never be solved fully but it can be minimized. Since 1990, many wireless security protocols have been designed and implemented, but none proved to be convincing with the security threats that come every day with new dangers to our systems and information.

So, depending on the business needs and requirements it is very much important to address wireless network security more efficiently. Wireless network has gained wide deployment due to numerous benefits such as user mobility, rapid and cheap installation, flexibility, scalability, and increased productivity it offers. In addition, rapid advances in this technology with improved capabilities which is seen in third generation (3G) and fourth generation (4G) wireless devices make it attractive for enterprise to run their business. However, the use of this novel technology does not go without security risk. 802.11 networks also referred to as WLAN is challenged by lack of physical protection in the medium.

Moreover, the fact that WLAN device are ship with all security features disabled make it a playground for hackers to tread on. Higher percentage of these hacker use to access internet freely and others use it for malicious activities. Traditional WLAN that relies on WEP has security flaws that were revealed in FMS attack (2001), Korek attack (2004), PTW attack (2007), and Chop-chop attack (2008), [3]. The consequences of unsecured WLAN are very dangerous to users and business enterprise. Attacks pepertrated on the networks have adverse effects on both individual users and business enterprises.

Network security [4] consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains:

It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Cryptography is the science of writing in secret code. More generally, it is about constructing and analyzing protocols that block adversaries; [5] various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation [6] are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering.

Applications of cryptography include ATM cards, computer passwords, and electronic commerce. The development of the World Wide Web resulted in broad use of cryptography for e-commerce and business applications. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Techniques used for decrypting a message without any knowledge of the encryption details fall into the area of cryptanalysis. Cryptanalysis is what the layperson calls "breaking the code." The areas of cryptography and cryptanalysis together are called cryptology. Encryption is the process of converting ordinary information (called plaintext) into unintelligible text (called ciphertext). Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. Cryptosystem is the ordered list of elements of finite possible plaintexts, finite possible ciphertexts, finite possible keys, and the encryption and decryption algorithms which correspond to each key.

The rest of the paper is organized as follows. In section II a survey on various secure authentication is explained. The Section III limitations of existing methods. The Section IV presents comparisons of existing methods and ends with conclusion in Section V.

II. REVIEW OF LITERATURE

Authentication is the gateway to a secure system. Along with the integrity, confidentiality and authorize it helps avoid any interference in the system. Until a few years ago was based authentication password again is the most common form of authentication for each network secure. However, with the advent of more sophisticated technologies that forms of authentication, although not yet become widespread unsafe. Moreover, with the increase of the "Internet of things" in which the number of devices grow collector, it would not be feasible to remember countless passwords for users It is therefore important to resolve this concern by drawing paths, where multiple forms of authentication are required to access all intelligent devices and also the ability to use would be high. [7]

In [10], The B-R algorithm is also a mixer of Blowfish and RC6. It is also a 128 bit algorithm and the algorithm uses two S-boxes with 259 entries each. But this algorithm's time complexity is too large because in every iteration it uses two functions: one is Blowfish function and the other is RC6 function and it also contains the risk of reflectively weak key attack and collision key attack for using the same function and two s-boxes.

In [9], a comparison is made that proved Blowfish takes minimum encryption + decryption time that may be helpful for Wi-Fi but this paper did not discuss anything about its security. In [8], four cases were shown by mixing and changing the number of the XOR and addition function of 'F' function but this does not able to remove the reflective and collision attack. The interesting approach to access control was proposed in [11] where researchers encrypted secret documents with separate tags inside the document to allow only authorized parties to access certain portions of the document. The biggest drawback in the system is the key management - once the key is given, it is hard to revoke it. It is also only applicable to electronic documents and does not involve location validation.

M. Umaparvathi et.al (2010) discussed the comparison of the most commonly used symmetric encryption algorithms AES (Rijndael), DES, 3DES and Blowfish in terms of power consumption. A comparison has been conducted for those encryption algorithms at different data types like text, image, audio and video. Results showed that AES has a better performance than other common encryption algorithms used. Since AES has not any known security Weak points so far, this makes it an excellent candidate to be considered as a standard encryption algorithm. 3DES showed poor performance results compared to other algorithms since it requires more processing power [12].

Tingyuan Nie et.al (2010) discussed the performance of two symmetric key encryption algorithms: DES and Blowfish which commonly used for network data encryption. In this paper, they analyzed encryption security, evaluated encryption speed and power consumption for both algorithms. Experimental results show that Blowfish algorithm runs faster than DES, while the power consumption is almost the same. It is proved that Blowfish algorithm maybe more suitable for wireless network which exchanges small size packets [13].

Cabernet [15] is a system for providing moving vehicles Internet access using Wi-Fi APs. However, Cabernet only provides intermittent network connectivity with the current Wi-Fi deployment density. As a result, Cabernet is only viable for non- or low-interactive applications, such as emails and web browsing. A recent measurement study on 802.11 wireless channels [16] shows that the mobility of users results in highly dynamic wireless links, which can significantly affect the performance of mobile applications.

A channel-aware rate adaptation algorithm is developed in to help select the transmission rate of a Wi-Fi connection. The above studies have shown that the unplanned Wi-Fi networks are only viable for the applications that can tolerate intermittent connectivity.

Wang et al. [16] proposed Wi-Fi deployment algorithms based on realistic mobility characteristics. Even though their algorithms significantly improve the continuous coverage for mobile users while reducing the required number of APs, they regarded Wi-Fi as a separated network and did not consider the objective of mobile data offloading. Quantum cryptography is described as a point-to-point secure key generation technology that has emerged in recent times in providing absolute security. Researchers have started studying new innovative approaches to exploit the security of QKD for a large-scale communication system. A number of approaches and models for utilization of QKD for secure communication have been developed. The uncertainty principle in quantum mechanics created a new paradigm for QKD [17].

One of the approaches for use of QKD involved network fashioned security. BBN DARPA quantum network is an example of such network. Researchers at Boston, Harvard University, and BBN technologies jointly developed the DARPA Quantum Network in 2004. The main goal was point-to-point Quantum network that exploited QKD technology for end-to-end network security via high speed QKD.

802.11i pre-authentication scheme is to reduce the authentication time in 802.11i WLAN, the IEEE 802.11 work group has already defined the 802.11i pre-authentication scheme, in which the client will previously authenticate with other neighbouring APs through the current connected AP. Through this pre-authentication, a key called pair-wise master key (PMK) is generated and held by both the CL and the pre-authenticated AP, and after the CL handoffs to one of the pre-authenticated APs, it does not need to do a full authentication but just a short four-way handshake key negotiation based on the pre-generated PMK. In this way, the handoff delay is significantly reduced meanwhile the secure level is not sacrificed much [18].

III. LIMITATIONS

- It uses an extensible authentication protocol over LAN (EAPOL) frames in the MAC layer which means that all the protocol frames and packets are transferred and directed by MAC address, so it needs the APs to be connected in the same LAN or through bridges or a distributed system. This limits the scalability of pre-authentication, and it is hard to use them in multi-hop networks, for example, wireless mesh networks and other IP routing-based networks.
- It works only in the same domain, that is to say that cross-domain operation is not supported. The reason we consider multi-domain operation is because there exist many Wi-Fi networks deployed in the same area. Moreover, end users may be able to access more than one of them, so if we can make use of multiple networks that belong to different domains, it would benefit both end users and network owners.

IV. COMPARISON OF EXISTING METHODS

Reference number	**Algorithm or method**	**Advantage**	**Disadvantage**
10	B-R algorithm	also contains the risk of reflectively weak key attack and collision key attack for using the same function and two s-boxes	time complexity is too large because in every iteration

12	symmetric encryption algorithms : AES (Rijndael), DES, 3DES and Blowfish	AES has a better performance than other common encryption algorithms used	3DES showed poor performance results compared to other algorithms
13	two symmetric key encryption algorithms: DES and Blowfish	Blowfish algorithm maybe more suitable for wireless network which exchanges small size packets	Blowfish algorithm runs faster than DES, while the power consumption is almost the same
16	Wi-Fi deployment algorithms	improve the continuous coverage for mobile users	did not consider the objective of mobile data offloading
18	802.11i pre-authentication scheme	reduce the authentication time in 802.11i WLAN	hard to use them in multi-hop networks, for example

V. CONCLUSION

Wi-Fi has a notoriously weak security standard. Wi-Fi security is not an easy task. Wireless network security is more difficult than wired network security. The main goal of this survey work is to shows existing method to improve the security aspect of WLANs. It has been shown that the integration of Cryptography in Wireless Networks has great prospective in terms of better network security. This paper discussing various methods used in Wi-Fi system for security purpose that improves the communication enhancement.

REFERENCES

[1] Paul Arana, INFS 612 – Fall 2006 “Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)”, "IEEE 802.11i." Wikipedia, The Free Encyclopedia. 11 Nov 2006, 10:22 UTC. Wikimedia Foundation, Inc. Nov. 25 2006
[2] “Understanding the updated WPA and WPA2 standards”.ZDNet Blogs. Posted by George Ou. June 2 2005. http://blogs.zdnet.com/Ou/?p=67
[3] Beck, M. and Tews. E. (2009). Practical Attacks Against WEP and WPA. Available: http://dl.acm.org/citation.cfm?id=1514286.
[4] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317-323.
[5] Davis, R., “The Data Encryption Standard in Perspective,” Proceeding of Communication Society magazine, IEEE, Volume 16 No 6, pp. 5-6, Nov. 1978.
[6] S. NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 200
[7] Gupta, U., (20 Jun 2015),“Application of Multi factor authentication in Internet of Things domain”, Information Networking Institute Carnegie Mellon University, Pittsburgh – Pennsylvania, USA, Volume 2, 1 – 6, web [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1506/1506.03753.pdf, [Access Date: 05/08/2016]
[8] Vaibhav Poonia, Dr. Narendra Singh Yadav, ” Analysis of modified Blowfish Algorithm in different cases with various parameters”, International Journal of Engineering Research and General Science, Volume 3, Issue 1, ISSN 2091-2730, January-February 2015.
[9] Gurjeevan Singh, Ashwani Kr. Singla, K.S. Sandha,” Superiority of Blowfish Algorithm in Wireless Networks”, International Journal of Computer Applications, Volume 44, No.11, pp-0975 – 8887, April 2012
[10] Janan Ateya Mahdi, ”Design and Implementation of Proposed B-R Encryption Algorithm” ,IJCCCE, VOL.9, NO.1, 2009.
[11] Burnap and J. Hilton, “Self protecting data for deperimeterised information sharing.” in ICDS. IEEE Computer Society, 2009, pp. 65–70
[12] M.Umaparvathi, Dr.Dharmishtan and K Varughese (2010), “Evaluation of Symmetric Encryption Algorithms for MANETs”, Proceedings of 2010 IEEE International conference on Computational Intelligence and Computing Research (ICCIC-2010), 28-29 Dec. 2010, pp 1-3.
[13] Tingyuan Nie, Chuanwang Songa and Xulong Zhi (2010), “Performance Evaluation of DES and Blowfish Algorithms”, Proceedings of 2010 IEEE International Conference on Biomedical Engineering and Computer Science (ICBECS- 2010), 23-25 Apr 2010. pp 1-4.
[14] V. Bychkovsky, B. Hull, A. Miu, H. Balakrishnan, and S. Madden, “A measurement study of vehicular internet access using in situ wi-fi networks,” in Proceedings of the 12th annual international conference on Mobile computing and networking, 2006.
[15] J. Eriksson, H. Balakrishnan, and S. Madden, “Cabernet: vehicular content delivery using wifi,” in Proceedings of the 14th ACM international conference on Mobile computing and networking, 2008
[16] G. Judd, X. Wang, and P. Steenkiste, “Efficient channel-aware rate adaptation in dynamic environments,” in Proceeding of the 6th international conference on Mobile systems, applications, and services (Mobisys08), 2008
[17] Elliott, C., “The DARPA Quantum Network”, Quantum Communications and Cryptography, 2006.
[18] RFC3748: ‘Extensible authentication protocol (EAP)’, 2004
[19] Tian Wang, Guoliang Xing, Minming Li, and Weijia Jia, “Efficient WiFi Deployment Algorithms based on Realistic Mobility Charateristics,” IEEE MASS, 2010.