A Unique Wireless Device Fingerprinting Technique for Secured Data Communication in Wireless Network

Murali Kotha
Student – B.Tech
Dept. of CSE
JNIT, Hyderabad.

Madhavi Singirikonda
Student – B.Tech
Dept. of CSE
JNIT, Hyderabad

Madhula Nirosha
Student – B.Tech
Dept. of CSE
JNIT, Hyderabad

G. Manjunath
Head
Dept. of CSE & IT
JNIT, Hyderabad

ABSTRACT

Wireless network suffers from security threats which are of different nature. One of the most significant reasons for weak security of the wireless network is the lack of strong key exchange technique. In 802.11 adaptation of wireless protocol, generally end users selects the key for current session and exchange encrypted data with same key for extended period of time. As the basic keys are weak, it is highly vulnerable to attacks and the packets are easy to intrude/read/modify. In this work we propose a unique solution of generating a strong key fingerprint automatically from the device of the user and use the same as key. We consider file transmission security between an AP and STA where the STA is a mobile node. We demonstrate the effectiveness of the technique with the help of real time setup and by synthesizing attacks like MAC address duplicating, using duplicate SIM and packet injection. The system is tested with 800MB of data transmission under different scenario and has yielded a zero hacking success of the data. As the system does not require any special hardware or software for implementing the same, it is easy to adopt and is acceptably scalable.

Keywords

Packet Injection, MAC Spoofing, Wireless Device Finger Printing.

1. INTRODUCTION

Wireless device fingerprinting is a mechanism by means of which unique stream or string sequence can be generated from communicating wireless devices. There are several unique identifiers associated with every wireless device for example the MAC address of the Nic card that comes with the device, SIM card for GSM/CDMA devices, SSSID or node name, inbuilt device identification code and so on. When a suitable mechanism is architected, this information set can be used as a unique identifier which can be used as key or for authorization purpose.

As most of these keys are Alpha numeric in nature, this set forms an interestingly strong key which is way better than the user levels keys that are used for secured communication in such a network. A hybrid and commonly used wireless home network has different types of wireless devices like mobiles, laptops, sensors which share information and communicate through an Access points. Access points are basically fixed architecture nodes which are within the communication proximity of most of the devices. Generally laptops and personal computers are used as access points. There are different types of wireless interfaces like Bluetooth, GSM, ZigBee, WiMax which communicates in such a network. Some of the devices are human operated, for example a data or file transfer over Bluetooth and some are automated for example transmission of sensor data through ZigBee interface. Hence developing a unanimous security extension for such a network should take into account of basic hardware and software available within the infrastructure rather than relying on changed in firmware/hardware or software as suggested by some of the papers. In this work we demonstrate the use of the technique in a mobile-laptop Bluetooth interface based file transfer which can easily be extended to other interfaces. Fingerprints or the unique streams are extracted and formed in the application layer and the encryption is performed in the application layer which leaves the underneath protocol interface intact and unchanged.

2. RELATED WORK

A unique fingerprinting technique which accurately and efficiently identifies the wireless driver without modification to or cooperation from a wireless device is developed [1]. Based on Underlying Statistical learning concepts a new location discovery technique is introduced based on SVM to estimate the location of a mobile user[2]. A mobile phone based system that explores logical localization via ambience fingerprinting is proposed and the results shows 87% when all sensing modalities are employed[3]. [4] investigates the properties of the received signal strength reported by IEEE 802.11b wireless network interface cards. [5] demonstrates that users can be tracked using implicit identifiers, traffic characteristics that remain even when unique addresses and names are removed. [6] proposes a new fingerprinting technique that differentiates between unique devices over a Wireless Local Area Network (WLAN) simply through the timing analysis of 802.11 probe request frames. This can be applied to spoof detection, network reconnaissance, and implementation of access control against masquerading attacks [6]. Clock skews of wireless devices needs to be measured. [7] Proposes a method that uses more accurate clock to measure clock skews which considers new parameters the fitted line intercept, c and the jitter - to guage the reliability of measure skews. Fingerprinting is a technique that records vectors of received power from several transmitters, and later matches these to a new measurement to position the new user and nearest neighbor techniques proved to be better [8]. Stanford Wireless Analysis Tool (SWAT) is a software tool for characterizing wireless networks. Metrics such as temporal and spatial correlation help users understand how different protocols, such as opportunistic routing and network coding, behave in a given network[9]. The effectiveness of rate adaptation algorithms is an important determinant of 802.11 wireless network performance and an accuracy of 95 to 100% is achieved [10]. [11] Proposes a non-parametric Bayesian method to detect the number of devices as well as classify multiple devices in a unsupervised passive manner. Specifically, the infinite Gaussian mixture model is used and a modified collapsed Gibbs sampling method is proposed[11] Two new mechanisms for the detection of wormholes in sensor networks and also further analyzed the implications of device fingerprinting on the security of sensor networking protocols[12].

3. PROPOSED WORK

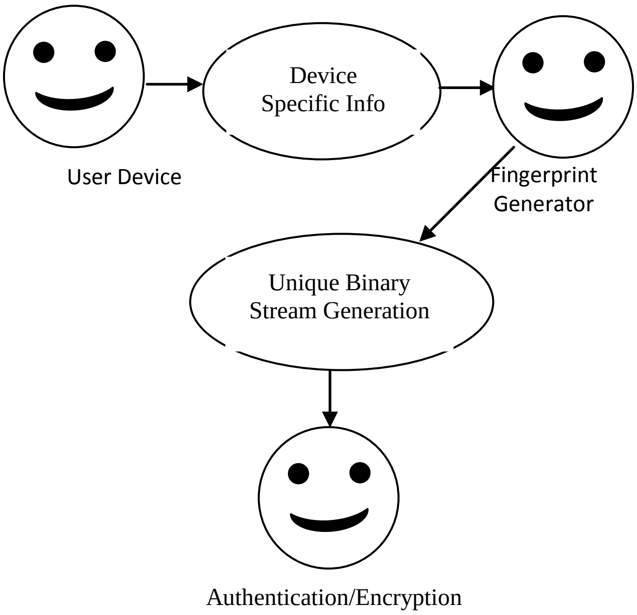


Fig 1. Use Case Diagram

Let us assume that a loptop is configured as an access point. When a mobile device requests an association through Bluetooth interface, access point extracts the MAC address and the SSID of the requesting device. Further it sends a connection request to the phone to get connected with Serial Port. Once both the devices are connected through the serial port , the phone operates as GSM modem and can respond to AT-Commands. Through AT-Command query, access point extracts the mobile number, sim card number and device PIN. Therefore even though common Bluetooth interface is used to exchange information, different ports and services are used which minimizes the security risk arriving from port scanning programs. Once all the keys are gathered, a unique key is generated from these keys and a file transfer request is responded with the files being encrypted with thus generated key slated with user level password. Files are decrypted at the mobile device through another application which fetches the information in the mobile and decrypts the information. In The Hand library for Bluetooth communication is used for access point centratic protocol design and J2ME based interface is developed for mobile centric interface.

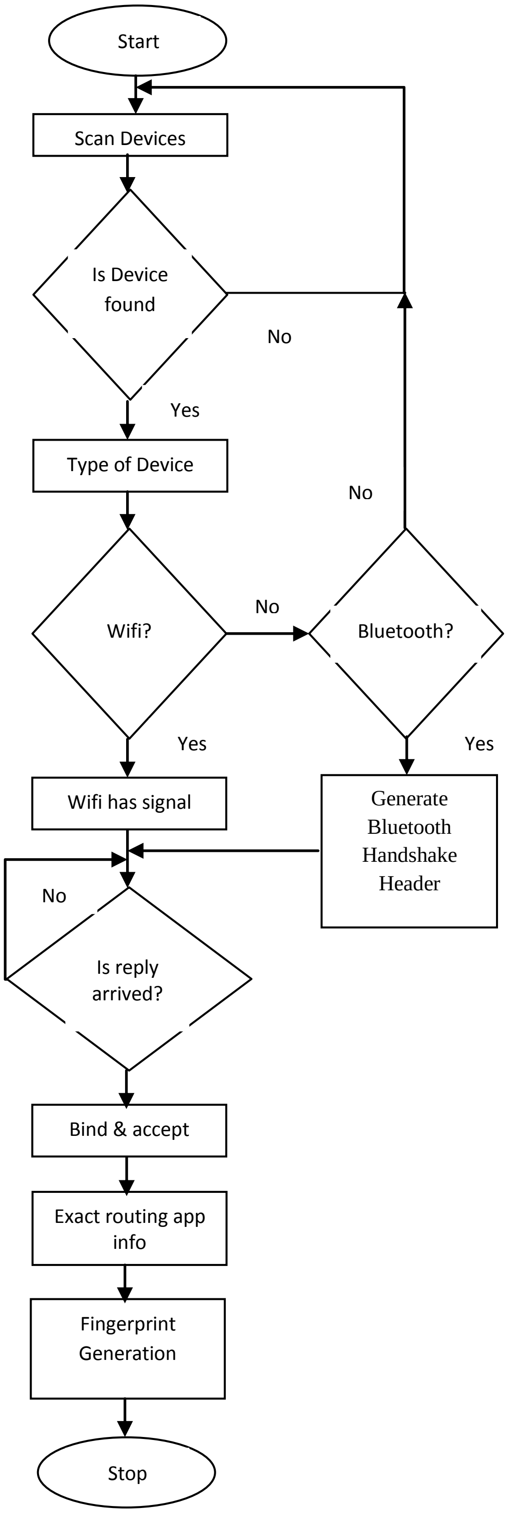


Fig 2. Flowchart of the System

RC4 based cryptosystem is adopted for the encryption which is explained as below.

RC4 generates a pseudorandom stream of bits (a keystream). As with any other binary cipher, which can be used for encryption by mixing it with the plaintext with the help of bit-wise or; decryption is performed the same way. (This is same as Vernam cipher except that generated PN bits, rather than a binary stream, is used.) In order to generate the key, the cipher makes use of a secret internal state which consists of two parts: (i) A combination of all 256 possible bytes (denoted "S" below).(ii) 2 8-bit pointers.

The combination is started with a variable length keystream, between 40 and 256 bits, with the help of the key-scheduling algorithm (KSA). Once it is completed, the stream of bits is generated using the pseudo-random generation algorithm (PRGA).

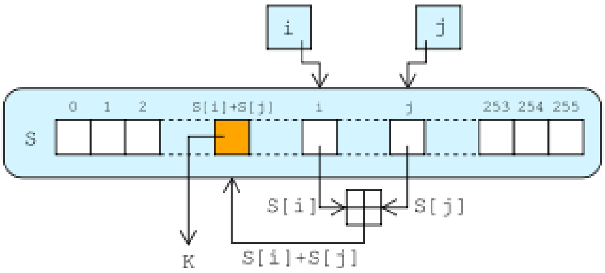
3.1 (KSA)

The key-scheduling technique is used to initiate the ombination in the S array. key length is defined as the number of bytes in the keystream and can be in the range 1 ≤ keylength ≤ 256, usually between 5 and 16, corresponding to a key length of 40 – 128 bits. First, the S is initialized to the identity permutation. Then S is subjected to different combinations.

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap values of S[i] and S[j]
endfor
```

3.1 The Pseudo –Random Generation Algorithm (PRGA)

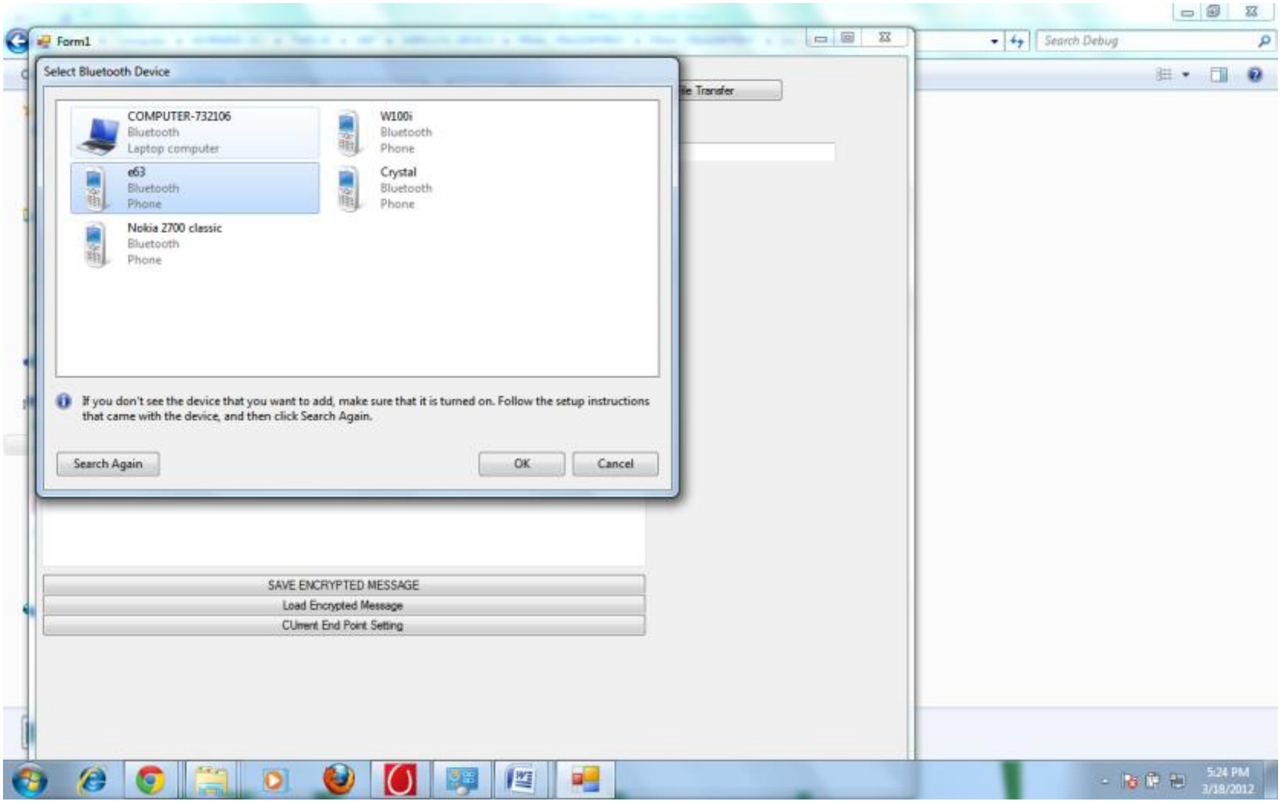
The lookup stage of the encryption technique. The output byte is selected by lookup table of the values of S(i) and S(j), adding them with mod256, and then looking up the sum in S; S(S(i) + S(j)) is used as a byte of the key stream, K.



For as number of iterations as are needed, the technique modifies the state and outputs a key byte. In each iteration, the algorithm increments i, adds the value of S pointed to by i to j, then exchange the values S[i] ,S[j], and then outputs the element of S at the location S[i] + S[j] (modulo 256). Each element of S is swapped with another element at least once every 256 iterations.

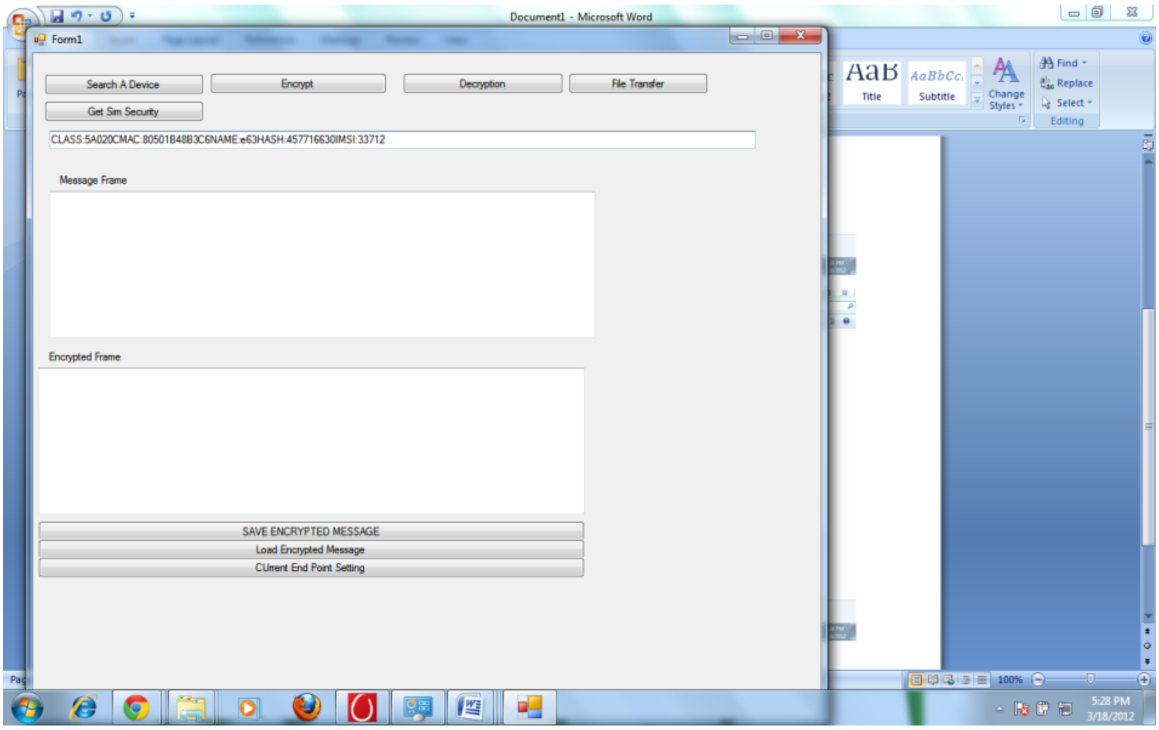
```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap values of S[i] and S[j]
    K := S[(S[i] + S[j]) mod 256]
    output K
endwhile
```

4. RESULTS



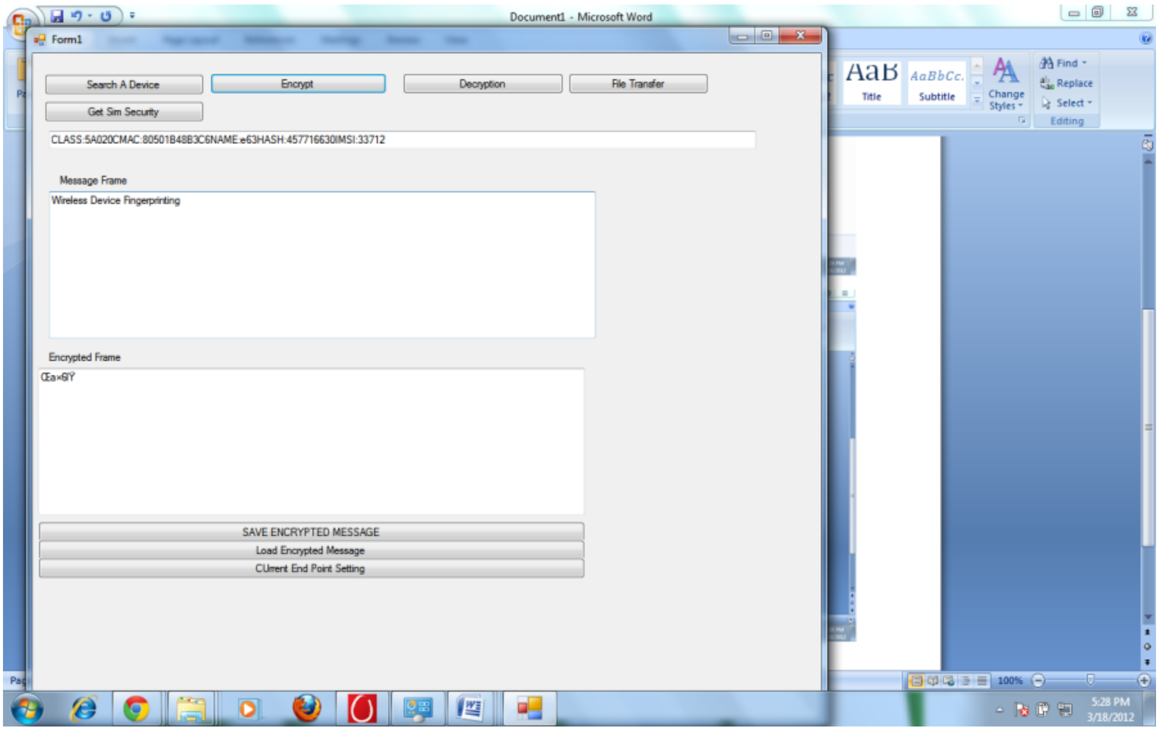
If you don't see the device that you want to add, make sure that it is turned on. Follow the setup instructions that came with the device, and then click Search Again.

Fig 3. AP selecting a STA for initiating a session



CLASS:5A020CMAC:80501B48B3C6NAME:e63HASH:457716630IMSI:33712

Fig 4. Generated Key from GSM and Bluetooth interfaces of the device.

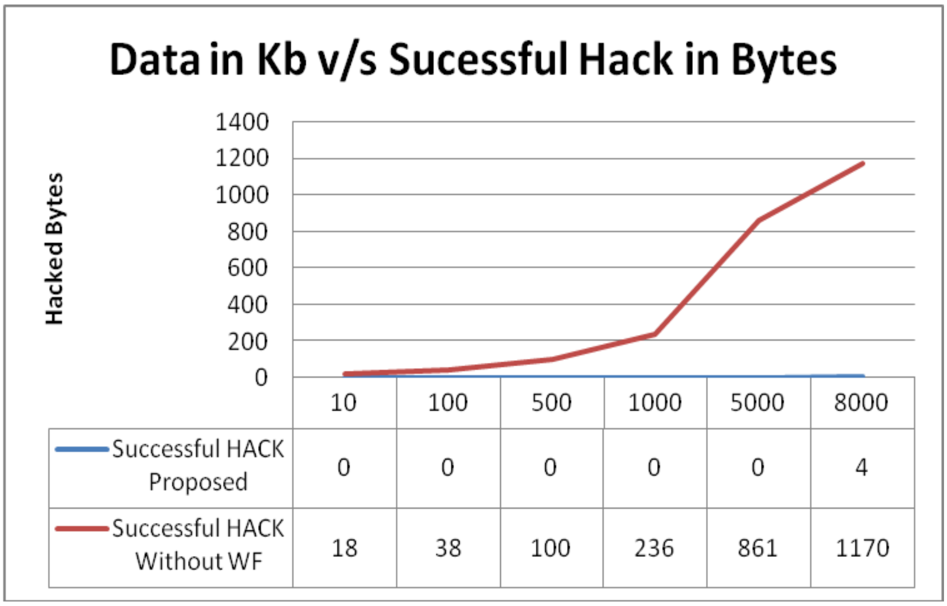


CLASS:5A020CMAC:80501B48B3C6NAME:e63HASH:457716630IMSI:33712

Message Frame: Wireless Device Fingerprinting

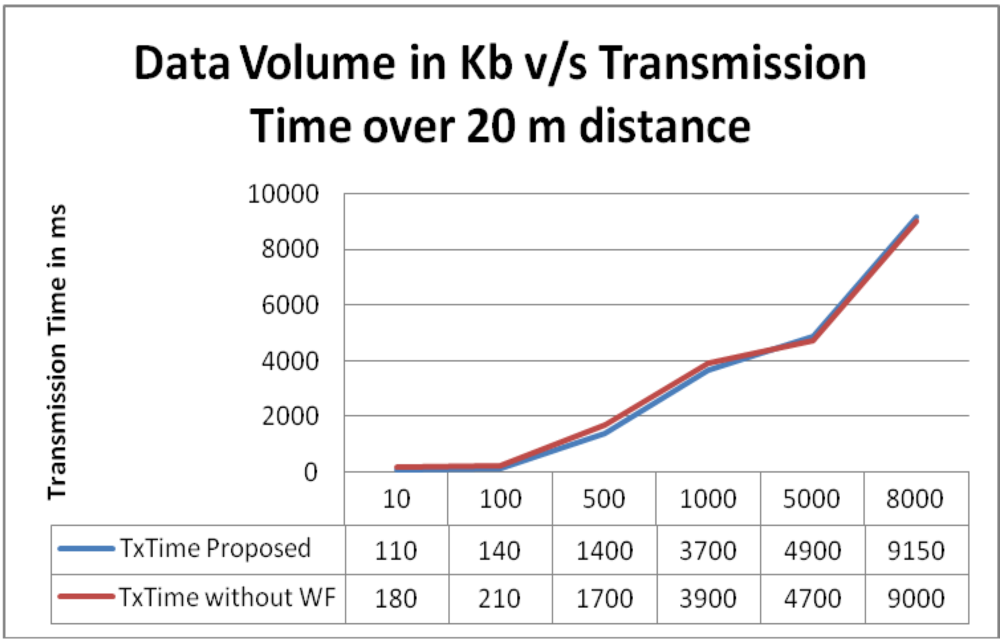
Encrypted Frame: Œa×6Ÿ

Fig 5. Result of Encryption



	10	100	500	1000	5000	8000
Successful HACK Proposed	0	0	0	0	0	4
Successful HACK Without WF	18	38	100	236	861	1170

Fig 6. Data Transmission volume in Session v/s Successful Hack with Random Keys



	10	100	500	1000	5000	8000
TxTime Proposed	110	140	1400	3700	4900	9150
TxTime without WF	180	210	1700	3900	4700	9000

Fig 7. Transimission time between two nodes in a distance of 20 meters

A Hacking process in initiated by capturing the wireless packets through wiresack and by random guess of the key. In each pass 1000 guesses of alpha numeric key is permitted. Sessions without proposed technique is secured through WEP where the session key is mutually selected by the end users. Figure 6 shows that the threat of data exposure is significant in wireless network if the key is weak. Therefore WEP enabled session's packets and data gets hacked with higher probability. But as wireless device fingerprinting allows better and stronger key, it offers far greater resistance against key guess.

Figure 7 Shows the transmission time between two nodes in a distance of 20 meters communicating with WEP and proposed technique. It clearly shows that transmission difference is minimum between packets that are encrypted with stronger key and packets that are not protected by strong keys. It also shows that for medium volume of data upto 500Kb(which is standard size of most of the images and files that are shared across Bluetooth), proposed technique delay is lesser than the packets encrypted with weak keys. It is due to the fact that strong encryption draws lesser subsequent hack attempts than the packets protected by weak keys. Hence WF automatically provides a faster and Secured environment.

5. CONCLUSION

Wireless Device fingerprinting is a terminology used to recognize wireless interfaces uniquely in a wireless interface. As oppose to it's wired counterpart, wireless packets traverses through insecure open air which makes the other interfaces to listen to the packets. If the packets and the data are not suitably encrypted, it welcomes far more attacks than a wired interface. Hence securing the packets through stronger keys are desirable. But as humans can not remember and hence cant use stronger keys, wireless communication remains prone to attacks. In this paper we have proposed a unique real time solution to secure the packets over wireless medium by securing data through stronger keys which are automatically generated from several interface identities of the device itself. The probability of duplicating every identity of a device, say SIM card, IMSI number, MAC address together is improbable. Hence the proposed technique offers real time protection to Home and enterprise network at the same time.

6. REFERENCES

[1] J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. Van Randwyk, and D. Sicker. Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting. Usenix Security Symposium, 2006.

[2] M. Brunato and R. Battiti, “Statistical learning theory for location fingerprinting in wireless LANs,” Comput. Netw., vol. 47, pp. 825–845, 2005.

[3] M. Azizyan, I. Constandache, and R. Roy Choudhury, “Surround-Sense: Mobile Phone Localization via Ambience Fingerprinting,” Proc. 15th ACM MobiCom, 2009, pp. 261–72.

[4] K. Kaemarungsi and P. Krishnamurthy, ”Properties of indoor received signal strength for WLAN location fingerprinting”, Proc. 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous ’04), Boston, Mass, USA, August 2004, pp. 14-23.

[5] Jeffrey Pang, Ben Greenstein, Ramakrishna Gummadi, Srinivasan Seshan, and David Wetherall. 802.11 user fingerprinting. In MobiCom ’07: Proceedings of the 13th annual ACM international conference on Mobile computing and networking, pages 99–110, New York, NY, USA, 2007. ACM.

[6] C. C. Loh et al., “Identifying unique devices through wireless fingerprinting,” in Proc. of the first ACM conference on Wireless network security, Mar. 2008, pp. 46–55.

[7] C. Arackaparambil, S. Bratus, A. Shubina, and D. Kotz. On the Reliability of Wireless Fingerprinting Using Clock Skews. In Proceedings of the 3rd ACM Conference on Wireless Network Security (WiSec), 2010.

[8] Dempster, A.G.; Binghao Li; Quader, I., "Errors in Determinstic Wireless Fingerprinting Systems for Localisation", International Symposium on Wireless Pervasive Computing, 2008.

[9] Kannan Srinivasan, Maria A. Kazandjieva, Jung Il Choi, Edward S. Kim, Mayank Jain, and Philip Levis, “SWAT: Fingerprinting Your Wireless Network”, Demo at SIGCOMM 2009.

[10] Mirza, M.; Barford, P.; Xiaojin Zhu; Banerjee, S.; Blodgett, M.; "Fingerprinting 802.11 rate adaption algorithms ", Proceedings of IEEE Infocom, 2011.

[11] Shan Kang; Naiwen Chen; Mi Yan; Xiaoxiao Chen; "Detecting identity-spoof attack based on BP network in cognitive radio network ", in: Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2011.

[12] K.B. Rasmussen and S. Capkun. Implications of Radio Fingerprinting on the Security of Sensor Networks.Proceedings of IEEE SecureComm, 2007.