Comparison of Cross Layer Techniques for Wireless Network Security for 802.11

Priya Pradeep Bhirud
M.E. Computer Engineering Department, Mumbai
K.J.Somaiya College of Engineering, Mumbai
Mumbai University, India.

Abstract:
Wireless technology has been gaining popularity over some years. Adaptation of standard depends on ease of use and level of security it provides..In this paper, we will study and compare Security techniques to detect attack in 802.11 by fusing multi-layer metrics is presented. We will discuss advantages and limitations of techniques of cross layer approach for wireless network security. Cross-layer approach has gained interest in performance optimization due to their design advantages.

Keywords:
Dempster-Shafer, wireless attacks, Wi-Fi, WEP, WPA, TKIP, PSK, Wireless Security.

1. INTRODUCTION
Wireless communication networks are becoming susceptible to more sophisticated and untraceable attacks. Network monitoring tools, such as Intrusion Detection Systems (IDS), have been developed for the purpose of detecting such attacks. Most of these tools are not efficient enough because they either focus on just one layer of observation (i.e. MAC layer) or use a limited number of metrics without properly combining each metric. A simple algorithm that utilizes a single metric from one layer may give positive results for detecting attacks in some cases. However, this single metric method might lack efficiency in many other cases, where the nature of the selected metric might conceal the actual attack. As a result, the performance of a single metric algorithm is poor with an unacceptable number of false alarms. Therefore, a cross-layer approach may offer a collaborative decision among layers, potentially resulting in higher detection accuracy rate and lower number of false negative (FN) and false positive (FP). Hence, utilizing a cross-layer approach may help towards automating the overall process of detecting and mitigating wireless network attacks.

This describes the methodology of using metrics from multiple layers of Wireless Communication Networks for detecting wireless security attacks and particularly Man-In-the-Middle (MitM) attacks at the physical layer. The metrics are analysed and compared to historical data and each gives a belief of whether an attack takes place or not. The beliefs from different metrics are combined with the Dempster-Shafer (D-S) theory of evidence method with the ultimate goal of limiting false alarms and improving the overall performance. D-S theory of evidence method is a mathematical framework for the representation of uncertainty. The aim of our methodology requires the system to be of low cost, scalable and applicable to other wireless technologies apart from the tested IEEE 802.11 standard. The presented methodologies have been evaluated by having an attacker inject forged replies to the HTTP queries of a victim while accessing four different websites. The number of FP and FN results are counted and compared against techniques that utilize only single metrics. We compare our collaborative approach against results by methods using single metrics and combination of two metrics.

1.1Organization of report

In this report in literature survey, we will be discussing overview of various wireless security techniques. We will study new technique for Wi-Fi security using fusion of multi-layer metrics for attack detection for single layer matrix, two layer matrix and three layers i.e. cross layer matrix. In results section result of comparison will be stated down.

2. LITERATURE SURVEY

The IEEE 802.11standard describes wired equivalent privacy (WEP) that defines a method to authenticate users and encrypt data between the PC card and the wireless LAN AP (Access Point). In large enterprises, an IP network level security solution could ensure that the corporate network and proprietary data are safe. Virtual private network (VPN) is an option to provide remote employees with secured access to employer's internal network. Since hackers are getting smarter, it is imperative that wireless security features must be updated constantly. Wireless network standards and some of the common security protocols are reviewed in brief.

1. WEP

Wired Equivalent Privacy, or WEP, authentication scheme requires each frame to be encrypted using an RC4 stream cipher that is decrypted upon arrival at the access point. It is only good for data sent between access points (wired networks don't and can't use WEP . To encrypt the data, WEP uses a seed that takes a shared secret key (the "WEP key") and combines it with a 24-bit piece of data called the initialization vector. The vulnerability is the static shared secret keys[15]. Since keys can't be exchanged among access points in the network, the same keys are used for extended periods of time.

2. WPA

Wi-Fi Protected Access (WPA) is a security standard for users of computers equipped with Wi-Fi wireless connection [19]. It is an improvement on and is expected to replace the original Wi-Fi security standard, Wired Equivalent Privacy (WEP). WPA provides more sophisticated data encryption than WEP. WEP is still considered useful for the casual home user, but insufficient for the corporate environment where the large flow of messages can enable eavesdroppers to discover encryption keys more quickly. WPA's encryption method is the Temporal Key Integrity Protocol (TKIP)[15]. TKIP addresses the weaknesses of WEP by including a per-packet mixing function, a message

integrity check, an extended initialization vector, and a re-keying mechanism.

3. WPA-PSK and WPA-Enterprise

WPA-PSK is a simplified but still powerful form of WPA most suitable for small business and home office networking . To use WPA-PSK, a person does set a static key initially, like with WEP. But WPA uses TKIP and automatically changes the keys at a preset time interval. This makes it more difficult for hackers to find and exploit them. So while there is still a static key, it is much more difficult to find and break.

4. 802.11x

802.1x is an authentication standard that provides an authentication for 802-based LANs [3]. 802.11x is a portbased network access control. Until a port is authenticated, it can only be used to pass traffic associated with the authentication process. Authentication is managed at a centralized authentication server. In addition, 802.11x has an option, ability, for distributing keys. This ability to distribute keys corrects the WEP's failings. To carry an authentication message it specifies the Extensible Authentication Protocol (EAP). EAP can carry number of actual authentication protocols (EAP-TLS, EAP-OTP).

In Wireless Local Area N/Ws, privacy is achieved by data contents protection with encryption. Encryption is optional in 802.11 WLANs, but without it, any other standard wireless device, can read all traffic in network. There have been three major generations of security approaches, which is mentioned below:

• WEP (Wired Equivalent Privacy)
• WPA (Wi-Fi Protected Access)
• WPA2/802.11i (Wi-Fi Protection Access, Version 2)

2.1. Dempster-Shafer Theory

B. Mathematical Framework

Dempster-Shafer theory method is a discipline of mathematics that combines evidence of information from multiple and heterogeneous events in order to calculate the probability of occurrence of another event.

The D-S theory starts by assuming a Universe of Discourse $\Theta=\{\Theta_1,\Theta_2,\Theta_3,\ldots\ldots\Theta_n\}$also called a Frame of Discernment, which is a finite set of all possible mutually exclusive propositions and hypotheses about some problem domain. With regards to this work, the frame of discernment is With regards to this work, the frame of discernment is comprised of *A* = "*Attack*" and *N* = "*Normal*". Assuming Θ has two outcomes {*A*, *N*}, the total number of subsets of Θ defined by the number of hypotheses that it composes, is $2^{\Theta}=\{A,N,\{A/N\},\emptyset\}$

Each proposition (subset) from _ is assigned a probability or a confidence interval within [0, 1], by an observer from the mass probability function Θ also known as the basic probability assignment:

$$m : 2^{\Theta} \rightarrow [0,1] \quad if \quad \begin{cases} m(\emptyset) = 0 \\ m(A) \geq 0, \forall A \subseteq \Theta \\ \sum m(A) = 1 \end{cases}$$

The function m(A) is defined as *A*'s basic probability number. It describes the measure of belief that is committed exactly to hypothesis *A*. In order to define the confidence interval that is given to a certain event, two functions must first be defined. These are the Belief function (*Bel*) and the Plausibility function (*Pl*). The former is a belief measure of a hypothesis *A*, and it sums the mass value of all the non-empty subsets of *A*.

$$Bel(A)=\sum m(B) \quad \textit{for all values of A subset of } \Theta$$

The doubt function (*Dou*) is given by

$$Dou(A)= Bel(\neg A) = 1- \sum m(B)$$

which accounts for all evidence that rule out the given proposition represented by *A*.

Similarly, the *Pl* function takes into account all the evidence that does not rule out the given proposition. In other words, it expresses how much we should believe in *A* if all currently unknown facts were to support *A*.

$$Pl(A)=1 - Dou(A)$$

Thus, the true belief in hypothesis *A* will be along the interval [*Bel*(A), *Pl*(A)]. However, in practice, the values of the interval could be identical and therefore the interval becomes unique value.

The idea behind the D-S rule of combination is to fuse the belief from two different observers into one given hypothesis.

Table 1.Example event probabilities assigned by m1,m2

m_1/m_2	{A}:0.32	{N}:0.25	{A,N}:0.43
{A}:0.35	0.11	0.09	0.15
{N}:0.1	0.03	0.025	0.04
{A,N}:0.55	0.18	0.14	0.24

Let m_1 and m_2 be the basic probability assignments from observer 1 and 2 respectively. The cells in the above table represent the multiplication of the m_1. belief with the m_2 belief, horizontal and vertical axis, respectively.

Their orthogonal $m=m1 \oplus m_2$ is defined as

$$m(A) = \frac{\sum_{X \cap Y = A} m_1(X) * m_2(Y)}{1 - \sum_{X \cap Y = \emptyset} m_1(X) * m_2(Y)} \quad \forall A \neq \emptyset$$

If the denominator of eq. (1) is equal to zero then value of $K = 0$, then $m1 \oplus m_2$ does not exist and m_1 and m_2 are said to be totally or flatly contradictory. To easily understand how to apply the D-S algorithm, a real example from our measurements is presented. The basic probabilities for an event being "*Attack*", "*Normal*", and "*Uncertain*", can be tabulated as seen in Table I.
Firstly *K* is calculated from eq.(1):
1-(0.03+0.09)=0.88 Similarly, 1/K=1.136 As described in eq.(1), for any event E the combined belief is given by:

$$m(E)=(1/K) * \sum_{X \cap Y=E} m_1(X) * m_2(Y)$$

Therefore
m(A)=1.136 * (0.11+1.15+0.18)=0.5
m(N)=1.136 * (0.025+0.04+0.14)=0.233
m(A|N)=1.136 * (0.24)=0.272

According to the results, the hypothesis more likely to be true is *A*, with higher belief than the other hypotheses.
Among the different methods , the D-S theory of evidence was chosen as one data fusion method because it has uncertainty management and inference mechanisms analogous to our human reasoning process [11]. This means, D-S is able to combine evidence from multiple and heterogeneous sources.
In addition, it is suitable for detecting previously unseen attacks because it does not require a priori knowledge. In contrast, Bayesian requires a priori knowledge and does not allow allocation of probability to ignorance but only to an event being normal or abnormal [7].

3. METHODOLOGY

1. MitM attack at Physical Layer

The most common and straight forward method for an attacker to perform a MitM attack is to do first MAC spoofing, usually by performing an ARP poisoning attack (i.e. the attacker sends messages indicating that he owns a specific MAC address). This is a well known MAC layer attack. However, for the purposes of this work, a MitM attack at the physical layer as implemented by the Airpwn tool was examined. Airpwn takes advantage of the duration of time that a server requires to respond to web-page requests. In that lag time, it can inject its own content onto the wireless channel of an access point. For example, a client may request a page from wikipedia.org that takes, round-trip, approximately 13 ms. If an attacker near the victim is running the airpwn tool [14], it will see the legal client's request and immediately responds with its own HTML code. Due to the fact that there are no hops between the attacker and the victim, it takes the attacker much less time to respond. When the client receives the data, it will assume the original request was answered and process the injected code. Even though the attack is launched at the application layer by injecting an HTTP packet, the actual attack is practical only because there are no mechanisms in WiFi 802.11[8] to prevent a misbehaving node from injecting their own malicious code in the form of valid 802.11 frames. When the real and authentic HTTP packet arrives, the content will either be ignored, if the packet size is smaller than the injected packet, or partially displayed, if the size is larger than the injected. Using scripts, Airpwn injects carefully crafted response code that could cause harm of varying severity. Less dangerous effects to the victim could include replacing the adverts of a specific web site with different ones; more dangerous activity could include redirecting the victim web browser to a phishing type of web site.
In this experiments, two types of attacks were launched against the client. Both attack codes were default options in the Airpwn suite. We refer to these attacks as Attack 01 and Attack 02. In the first type of attack, the attacker eavesdrops the HTTP request frame from a client destined to a web server and then proceeds by injecting a forged frame. In this type of attack the forged frame contains HTML code that replaces the title of the authentic web page to a custom one .. In the second type of attack, the attacker listens for requests for images hosted on the web site and injects its own images . In addition, the attacker injects TCP reset frames so the client proceeds requesting the remaining objects of the web site.
As this type of MitM attack takes place at the physical layer, it cannot be detected with conventional MAC spoofing detection techniques. For example, one way to detect MAC spoofing is by sending an ICMP packet to the victim IP which would result in two addresses replying (the victim and the attacker)

2. Metrics and Testbed

The next task was to examine the actual manifestations of the Airpwn tool across different layers. Several metrics are identified that if appropriately used could give evidence of a MitM attack at the physical layer. These metrics are: The Received Signal Strength Indication (RSSI), the transmission rate (or injection rate), and the Time To Live value (TTL).
The TTL value is a metric of the IP layer, the transmission rate belongs to the MAC layer and finally the RSSI is related to the Physical layer. The testbed where the experiments took place can be seen in Fig. 3. It includes a client associated with an AP and accesses web pages hosted on the Internet across different geographical locations. The attack scenario consists of an attacker that launches the attack using the Airpwn tool and a third party node in passive monitoring mode that captures packets from this particular wireless network. The monitoring node and the attacker were running the Backtrack Linux operating system and all the devices except from the AP used Atheros chipset in their wireless cards. The AP is a Cisco Linksys model. WRT54GL.
It should be noted that the attacker was placed very close to the AP, around 1.5 meters apart. This positioning of the equipment made the detection of attacks much more difficult as the RSSI values of the attacker could become identical to these of the AP. The RSSI is a volatile value that depends on many factors such as distance, physical obstacles, WLAN equipment, used frequency and an environmental coefficient. As a result, just by examining the RSSI values it could be difficult to differentiate between attacker and AP.
In addition, Airpwn does not dynamically adapt the TTL field of the injected frames but predefines it to a static random value. The Airpwn source code has a default TTL value of 255. As this value is quite unrealistic and could easily reveal which frames are malicious, the code was modified in order to change the TTL value to 64. This value was chosen because it is the default TTL value for Linux web servers and the injected frame could be misidentified as a frame of the local area network. The proposed methodology can be seen as

a flow chart in Fig. 4. By using a wireless monitoring node the packets transmitted are collected from both the authentic AP and the forged attacker. From the information within the packets, historical data are constructed for a specific time window. More specifically, the statistical mode of RSSI and TTL are calculated for the current window. The metrics RSSI and TTL from every received packet are compared against the mode of the current time period. The beliefs for "Attack" for each of the selected metrics are chosen experimentally and intuitively i.e. the bigger the difference from the mode, the higher the belief in the attack. Regarding the injection rate, a different approach was followed. Given that most attacking tools that inject forged packets are more efficient at low injection rates, a higher belief in attack was assigned for packets transmitted with a low rate and a lower belief in attack for packets transmitted with high rate.

Following figure1. Shows test bed and steps of Airpwn attack and figure 2 shows methodology for calculating cross layer metric values.

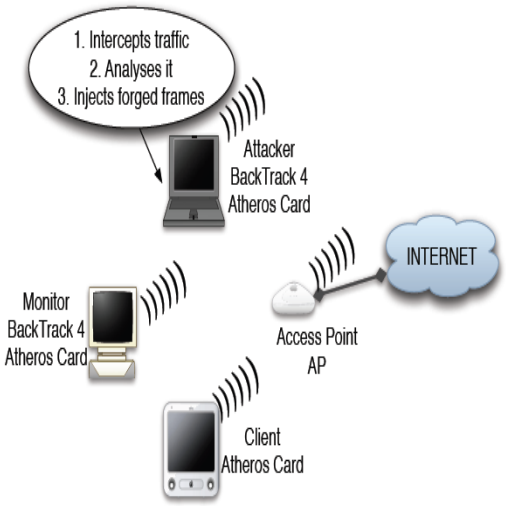

Figure1.Test bed and steps of Airpwn attack

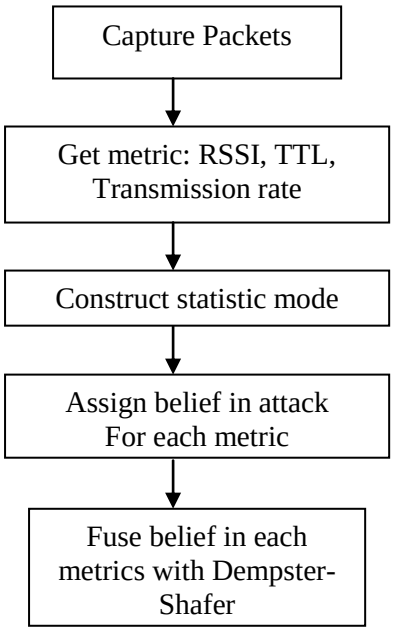

Figure2: Flowchart of Methodology

4. PRACICAL RESULTS AND DISCUSSION

In this results from the proposed cross-layer methodology are presented and compared against single layer metrics and against the cross-layer technique using just two metrics. The experiments were run while a client was accessing websites located in China, Spain, UK and US. The cross-layer results are presented in Table 2 and are the best results overall and for each individual experiment except for some FN results that occur while launching the second type of Airpwn attack when the client visits the Chinese and UK websites. These FN results occur because the RSSI and the TTL values of the attack packets coincide with the values of the estimated mode. This could happen because consecutive injected forged packets alter the actual value of the mode. As a result, both RSSI and TTL values of several attack packets are close to the mode, leaving the decision of whether an attack is happening or not just on the injection rate. However, the belief of an attack happening just by examining the injection rate is not high enough to raise an alarm. There is a trade-off between the number of FN and FP results of the algorithm and, therefore, increasing the belief in "Attack" for injection rate could reduce FN but would also increase FP.

The results for the single layer metrics RSSI and TTL are presented in Tables III and IV respectively. The RSSI has a high number of false alarms in most of the experiments. In particular, using just the RSSI metric the FN results are so high rendering this metric unacceptable for this purpose.

In the case of single metric TTL (Table IV), the results for FN are much less than results of the RSSI metric and the performance in terms of FN is similar to the one achieved by the cross layer technique But there is a big increase in the FP results in most of the cases. The combination of RSSI and injection rate metrics (Table V), quite surprisingly, results in bad performance in most cases with an extremely high FN percentage reaching even 100% in one case. This is a clear example showcasing that two metrics alone might not necessarily yield an improved performance and a more expanded synergistic approach from more metrics is necessary.

In the case of the combination of injection rate and TTL (Table VI), the performance is better in comparison to all single metrics. However,[given the overall high number of FP, especially for "US attack", its performance does not reach that level gained from the cross-layer results neither the one of the combination of RSSI and injection rate.

Table2
Single Metric Result Utilizing RSSI

Website	Types	False Pos. .(%)	False Neg. (%)
CHINA	Normal Attack1 Attack2	7.14 1.31 2.9	0 20 90
SPAIN	Normal Attack1 Attack2	5 1.56 0	0 0 87.5
UK	Normal Attack1 Attack2	0 0.97 14.5	0 0 94.5
US	Normal Attack1 Attack2	17.64 46.87 0	0 0 94.11

Table3
Single Metric Results utilizing Time-to Live

Website	Types	False Pos. .(%)	False Neg. (%)
CHINA	Normal Attack1 Attack2	22.45 21.05 16.67	0 0 15
SPAIN	Normal Attack1 Attack2	0 53.12 0	0 0 0
UK	Normal Attack1 Attack2	1.95 0 8.33	0 0 18.52
US	Normal Attack1 Attack2	4.98 6.25 11.29	0 0 0

Table4
Dual Metric Results utilizing Injection Rate and RSSI

Website	Types	False Pos. .(%)	False Neg. (%)
CHINA	Normal Attack1 Attack2	0 0 0	0 0 80
SPAIN	Normal Attack1 Attack2	0 0 0	0 0 25
UK	Normal Attack1 Attack2	2.82 3.03 5.56	0 100 64.96
US	Normal Attack1 Attack2	0 18.75 1.1.2	0 0 88.23

Table5
Dual Metric Result Utilizing Time-To-Live and Injection Rate

Website	Types	False Pos. .(%)	False Neg. (%)
CHINA	Normal Attack1 Attack2	0 0 0	0 0 0
SPAIN	Normal Attack1 Attack2	0 0 0	0 0 0
UK	Normal Attack1 Attack2	19.74 0 13.58	0 0 0
US	Normal Attack1 Attack2	0.98 43.75 1.13	0 0 0

5. CONCLUSION

This states that the conventional approach of using single metrics for detecting attacks in wireless networks is sometimes inefficient, inaccurate and misleading. Similarly, techniques involving multiple metrics without utilising a proper data fusion technique lack efficiency. To this aim, the authors propose a new approach for detecting wireless network attacks, involving combining beliefs from sensors of multiple layers of observation and their belief is combined to produce a collective decision on whether an attack takes place or not. The beliefs from different metrics are combined with the Dempster-Shafer theory of evidence method with the ultimate goal of limiting false alarms and improving the overall performance[1]. For combining beliefs among multiple metrics from various layers, our work examined and implemented the D-S theory of evidence method, which is a mathematical framework for the representation of uncertainty.

In this work, it is compared on basis of demonstrated experiments on a real wireless network that combining beliefs from multiple metrics in various layers outperforms the efficiency and accuracy of single metrics. The cross-layer results are the
best results overall and for each individual experiment except for some FN results present in two cases (UK and China in "Attack 2" scenario). These FN results are produced because consecutive injected forged frames alter the perception of characteristics for "normal" traffic of the algorithm. Clearly, this is a conceptual issue inherent in window based algorithms.

6. REFERENCES

[1] Kyriakopoulos, Konstantinos G.; Aparicio-Navarro, Francisco j. ; Parish, David j. "Fusing multi-layer Metrics for detecting security attacks in 802.11 networks" Wireless Telecommunication Symposium 2011.Digital Object Identifier: 10.1109/WTS.2011.5960832 Publication Year: 2011

[2] Aparicio-Navarro, Francisco J; Kyriakopoulos,. ; Parish Konstantinos G David J.- "An On-line Wireles Attack Detection System UsingMulti-layer Data Fusion". Measurements and Networking Proceedings (M&N), 2011dgital Object Identifiere10.1109/IWMN.2011.6088478 Publication Year: 2011 , Page(s): 1 – 5

[3] K. Bicakci and B. Tavli, "Denial-of-service attacks and countermeasures in ieee 802.11 wireless networks," Computer Standards & Interfaces, vol. 31, no. 5, pp. 931–941, 2009

[4] P. Bahl, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill, "Dair: A framework for managing enterprise wireless networks using desktop infrastructure," in Proceedings of the Fourth Workshop on Hot Topics in Networking (HotNets). ACM, 2005

[5] Y. Sheng, G. Chen, H. Yin, K. Tan, U. Deshpande, B. Vance, D. Kotz, A. Campbell, C. McDonald, T. Henderson, and J. Wright, "Map: A scalable monitoring system for dependable 802.11 wireless networks, IEEE Wireless Communications, vol. 15(5), pp. 10–18, 2008.

[6] M. Raya, J. Hubaux, and I. Aad, "Domino: a system to detect greedy behavior in ieee 802.11 hotspots," in Proceedings of the 2nd international conference on Mobile systems, applications, and services. ACM, 2004, pp. 84–97.

[7] Q.Chen and U.aicklin ,"Anomoly detection using the Demster Sheher Method" in Poceeding of 2006 International conference on Data Mining, DMIN 2006 2006,pp.pp.232-240

[8] D. Yu and D. Frincke, "Alert confidence fusion in intrusion detection systems with extended dempster-shafer theory," in Proceedings of the 43rd annual Southeast regional conference-Volume 2. ACM, 2005, pp 142–147.

[9] Q. Chen and U. Aickelin, "Anomaly detection using the dempster-shafer method," in Proceedings of the 2006International Conference on Data Mining, DMIN 2006, pp. pp. 232–240.

[10] V. Chatzigiannakis, G. Androulidakis, K. Pelechrinis, S. Papavassiliou, and V. Maglaris, "Data fusion and algorithms for network anomaly detection: classification Third evaluation," in Networking and Services, 2007. ICNS. International Conference on. IEEE, 2008, p. 50.

[11] h.Wu,M. Siegel.R.stiefelhagen,and J.Yang,"Sensor fusion using Demster Shafer theory"in IEEE Instrumentation and Measerment Technology Conference.IEEE,21-23 May 2002

[12] G. Thamilarasu, S. Mishra, and R. Sridhar, "A cross- layer approach to detect jamming attacks in wireless ad hoc networks," in Military Communications Conference, 2006. MILCOM 2006. IEEE. IEEE, 2007, pp. 1–7.

[13] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "Sensor fusion using dempster-shafer theory," in IEEE Instrumentation and Measurement Technology Conference. IEEE, 21-23 May 2002.

[14] A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)Lashkari, A.H.; Danesh, M.M.S.; Samadi, **B.**Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on Digital Object Identifier: 10.1109/ICCSIT.2009.5234856 Publication Year: 2009 , Page(s): 42- 52

[16] "Airpwn sourceforge website," Website.