

PROACTIVE WIRELESS NETWORK MANAGEMENT SYSTEM

Field of the Invention

[0001] The present invention relates to a wireless network. In particular, the invention relates to a system and method for monitoring a wireless computer network that are connected to at least one access point/router/gateway.

Background

[0002] Unlike wired network, which requires physical connection to each device connected thereto, a wireless network is more vulnerable to network intrusions as the intruder does not need to physically connect to the network. It is possible for any devices within the coverage of the wireless network to connect thereto with the necessary authentication, if any. However, the common wireless protocols and encryption methods used for access authentication are prone to security breach. Several open source utilities such as Aircrack-ng, weplab, WEPCrack or Aircsnort can be used to break in to a secured wireless network.

[0003] Countless network security systems and methods are available in the market. Some may even require dedicated devices to be deployed to protect the wireless network. Most of these network security systems and methods require trained technical personals to operate it. Some may even require network surveillance on 24/7/365 basis. However, such network surveillance is not practical for small office/home networks (SOHO).

25

[0004] General SOHO usually relies on security features provided along with access points (including wireless access points) used for network protection. These features include the built-in encryption, MAC ID filtering, static IP address filtering, network traffic logging and etc. These features can generally be accessed through common web-browser, such as Internet Explorer, Mozilla Firefox, Safari, etc. by keying-in an IP address assigned to that access point in the URL bar. User or

30

administrator of the access point can then configure and control the access point via a graphical user interface shown by way of dynamic web pages. However, most common users are not equipped with the necessary skills and knowledge for configuring and managing the access point. The access point configurations and the network traffic
5 information are shown passively when the dynamic web pages are updated.

[0005] Known methods to solve the problem: owners are required to manually and periodically monitor Wireless LAN activities via web interface/monitoring programs provided by access point's manufacturers; or some security products provide
10 common graphic user interface to do Wireless devices scanning with limited Wireless LAN router control. These methods have some limitation: The existing access point web interface are generally designed for technical personnel which is generally not understood by and usable to common home wireless network user who are non-technical people. Even for technically trained personals, they require additional time in
15 learning different web interfaces for different brand/model of wireless access points. The existing router web interface is a device-centric monitor/control process. The owner needs a user-centric process monitor/control process to control users using his Wireless network.

20 **[0006]** HomeNet Manager marketed under Singleclick Systems is a third party software for managing and securing home network. HomeNet Manager performs a scan to discover all nearby devices, including access points by passively listening to surrounding IP data packets. The HomeNet Manager is able to identify a device manufacturer ID based on a MAC address of the devices. The HomeNet Manager
25 requires to manually rescan the wireless signal to update a list of devices connecting to the network. The HomeNet Manager uses a IP address conflict method for blocking a device connecting to a network. With this method, the HomeNet Manager broadcasts a same IP address that the device to be blocked is using, causing the device be decline by the network. Further, the HomeNet Manage issues an invalid IP address to the blocked
30 device to prevent the device to be connected to the network. This method however is only usable when the HomeNet Manager is active. When the HomeNet Manager is shut down, the blocked device can restore the connection with the network. Further,

when the IP address of a device to be blocked is set at a static IP address, HomeNet Manager may not be able to block the device due to the static IP address.

5 **[0007]** It is imperative that owners of wireless network, especially the home networks, are informed who are the connected users at a given time in a simple and user friendly manner.

Summary

10 **[0008]** In accordance with one aspect, the present invention provides a network management system for accessing an access point connecting at least one client device to form a network. The network management system comprises a software agent for residing at the at least one client device, the software agent is operable to search for hyper text language pages stored in the access point and to extract relevant data
15 regarding status of the network connections from the hyper text language pages and a graphical user interface for listing all client devices connecting the network based on the extracted relevant data, the graphical user interface comprises controls for authorizing or blocking client devices connecting to network via the access point. The software agent updates the relevant data automatically at a predefined time.

20

[0009] In accordance with one embodiment, the software agent may search for hyper text language pages with regular expression of relevant keywords. Yet, it is also possible that the software agent search for hyper text language pages via requests under HTTP protocols. In another embodiment, the software agent may extract the relevant
25 data regarding status of the client devices with regular expression of relevant keywords. Yet in another embodiment, the software agent may extract the relevant data regarding status of the client devices via requests under HTTP protocols.

[0010] In accordance with another embodiment, the network management
30 system may further comprise a device library for storing information regarding access point of different models. The information regarding access point of different models

may further include pointers for appropriate hyper text language pages and the data regarding connection status.

[0011] In accordance with a further embodiment, the relevant data may include
5 information regarding all the client devices connection status, a model and brand of the access point, a MAC address, a IP address and a device name of the client devices.

[0012] In accordance with yet another embodiment, the network management system may further comprise a user library that includes information of the client
10 devices authorized to connect to the network.

[0013] In accordance with another aspect of the present invention, there is provided a method of accessing an access point connecting at least one client device to form a network for managing the network connection. The method comprises
15 searching for a hyper text language page for logging on to the access point; logging on to the access point with user name and password; searching for other hyper text language pages stored in the access point; extracting relevant data regarding status of client devices connection from the hyper text language pages; listing all the client devices connecting the network on a graphical user interface based on the extracted
20 relevant data; authorizing or blocking client devices connecting to the network via the access point via the graphical user interface; and updating the relevant data automatically at a predefined time.

[0014] In accordance with one embodiment, the searching for the hyper text
25 language pages may be by way of using regular expression of relevant keywords. Yet, the searching for the hyper text language pages may be based on requests under HTTP protocols. In another embodiment, the extraction of the relevant data regarding status of the client devices may be by way of regular expression of relevant keywords. Yet in another embodiment, the extraction of the data regarding status of the client devices
30 may be based on requests under HTTP protocols.

[0015] In accordance with yet another embodiment, the method may further comprises storing information regarding access point of different models. The information regarding access point of different models may include pointers for appropriate hyper text language pages and the relevant data regarding connection status.

5

[0016] In accordance with a further embodiment, the relevant data may include information regarding all the client devices connection status, a model and brand of the access point, a MAC address, a IP address and a device name of the client devices.

10 [0017] In yet another aspect, the present invention provides a software agent for accessing access point for monitoring network connection status. The software agent is recited at network client devices, such as desktop computer or notebook computer. The user can use a single click to instruct a home wireless access point to block/reject any connected devices. The software agent is adapted to automatically scan and search for
15 hyper text language pages used for accessing configuration of the access point and extract network status data from the hyper text language pages.

Brief Description of the Drawings

20 [0018] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0019] FIG. 1 illustrates a computer network having a network management system in accordance with one embodiment of the present invention;

25

[0020] FIG. 2A exemplifies a screenshot for logging into the access point in accordance with one embodiment of the present invention;

[0021] FIG. 2B exemplifies a screenshot of the network management system in
30 accordance with one embodiment of the present invention;

[0022] FIG. 2C exemplifies a screenshot of a GUI window of the network management system in accordance with another embodiment of the present invention;

[0023] FIG. 3 is a block diagram showing the network management system in
5 accordance with one embodiment of the present invention;

[0024] FIG. 4 illustrates a flow diagram showing the network monitoring process in accordance with one embodiment of the present invention;

10 [0025] FIG. 5 illustrates a flow diagram showing a process for creating a new device entry for a device library in accordance with one embodiment of the present invention; and

[0026] FIG. 6 illustrates a flow diagram showing a detailed process for network
15 monitoring in accordance with one embodiment of the present invention.

Detailed Description

[0027] In line with the above summary, the following description of a number of specific and alternative embodiments are provided to understand the inventive features of the present invention. It shall be apparent to one skilled in the art, however that this invention may be practiced without such specific details. Some of the details may not be described at length so as not to obscure the invention. For ease of reference, common reference numerals will be used throughout the figures when referring to the same or similar features common to the figures.

10

[0028] FIG. 1 illustrates a computer network 100 having a network management system 110 in accordance with one embodiment of the present invention. The computer network 100 can be a small local area network that comprises an access point 112, a desktop computer 114, a laptop computer 116, a personal data assistance (PDA) 118. The devices 114, 116 and 118 are authorized devices that connected to the access point 112 to form the network. The desktop computer 114 is connected to the access point 112 via a network cable (a wired connection) while the laptop computer 116 and the PDA 118 are connected to the access point via wireless connections. Due to the wireless capability, it is possible for any other wireless equipped devices such as an intruder 150 located within the coverage of the access point 112 to access thereto, whether intentionally or unintentionally. Therefore, the access point 112 is required to be configured for security protection.

[0029] Still referring to FIG. 1, the access point 112 can be accessed via launching a web browser of anyone of the devices connected thereto. Different models of access point may have different configuration layouts/interfaces which may not be easy for users without any relevant technical background to configure and manage the same. Therefore, a network management system 110 is provided in any of the devices 114, 116 and 118 for configuring the access point 112 and managing the computer network 100. The network management system 110 is adapted to access any brand or model of the access point 112. In operation, the network management system 110

searches for the access point 112 that connecting the computer network 100. Once the access point 112 is found, the network management system 110 accesses the access point 112 and extracts the necessary information. A login window 201 as shown in FIG. 2A is shown to prompt for user name and password for accessing the access point 112. When the user name and password are verified to be valid by the access point 112, the network management system 110 accesses the access point 112.

[0030] FIG. 2B shows a screenshot of the network management system in accordance with one embodiment of the present invention. The screenshot shows devices connections and provides network access control via a simple graphical user interface. The screenshot comprises a connections window 212, a log display window 214, an intruder log button 216, a blocked log button 218 and an exit button 220. The connection window 212 displays all the devices connected to the access point 112. The connection window 212 lists at least a device user name, a device name, an assigned IP address, and a MAC address. The device user name, IP address and MAC address are stored in a user library of the network management system 110. For devices that were not found in the user library of the network management system 110, the device user name is shown "Unknown". The device name is a name of the device assigned by the device owner while the device user name is a name assigned by the user of the network management system 110. The IP address can be automatically assigned by the access point, or user defined IP. Which ever case it is, the IP address assigned to each device is unique within the network. The MAC address is the unique identifier to each device and can be obtained from the device. The device name and the MAC address are captured from the device when the device is connected to the access point 112. The list of devices showing on the connection window 212 is selectable for connection control. The log display window 214 displays the connection activities of the access point 112. The log display window 214 is updated automatically. The information displayed on the log display window 214 is archived as a log data. The log data is stored at the local computer running the network management system, of which user can access it anytime as desired. The intruder log button 216 is used to list a list of intruder devices or unknown devices accessed to the access point 112. The blocked log button 218 is used

to list a list of devices that are blocked for that network. When the intruder log button 216 or the blocked log button 218 is pressed, a separated window (not shown) will appear to display all the archived information. The exit button 220 can be used to quit the network management system.

5

[0031] FIG. 2C shows another screenshot of a GUI window 230 of the network management system in accordance with one embodiment of the present invention. The screenshot is shown when any one of the devices in the list of the connection window 212 of FIG. 2B is selected and executed. The executed is typically by way of double clicking the selected devices from the list via a pointing device. In the GUI window 230, the device name, the assigned IP address and the MAC address is shown on the screen. The user of the network management system can choose to authorize or block the selected device. A user name can also be assigned for easy reference. When the selected device is blocked by the user of the network management system, the selected device's MAC address will be added automatically into the Mac address filter list provided originally by the access point 112. When a device is selected to be blocked, the network management system accesses a MAC-address filtering list of the access point 112 and input the device ID (such as MAC address) into the access point 112 to block the device permanently. Since the device ID is stored in the access point 112, even when the network management system (or the device running the network management system) is shut down, the device to be blocked remain inaccessible to the access point 112 at all time. The MAC address of the blocked devices is also archived in the intruder log, which can be displayed via the network management system as shown in FIG. 2B.

25

[0032] In the embodiment above, the devices 114, 116 and 118 are provided by way of example, not limitation. It is understood that the access point 112 can have more other devices of different types to be connected thereto, such as tablet PCs, gaming consoles, VoIP phones, Internet Cameras and the like.

30

[0033] The access point 112 illustrates herewith in a wireless router that provide both wired and wireless connection to the devices 114, 116 and 118 to form the

computer network 100. It also integrated with a modem that allows the computer network 100 to connect to the Internet.

[0034] The present invention provides an intermediate user-friendly graphics
5 interface for remotely controlling the access point.

[0035] FIG. 3 is a simplified block diagram showing how the network
management system of the device 114 monitors the access point 112 in accordance with
one embodiment of the present invention. The access point 112 comprises an access
10 point information 312, a data query 314 and a HTTP server 316. The access point
information 312 comprises the network connection status information, access point
setting information, user information and etc. Depending on the device model, the
access point information 312 is provided in its proprietary format. These access point
information 312 can be presented by way of the web pages provided by the HTTP
15 server 316 which are accessible by way of extensible markup language, such as XML
and the like, via the data query 314. The web pages are preformatted and stored on the
access point 112 and when the web pages are opened or refreshed, the access point
information 212 is displayed on the web pages.

20 [0036] Still referring to FIG. 3, the network management system 100 comprises
a control agent 302 and a graphical user interface (GUI) 304. The control agent 302 is
adapted to establish connections with the HTTP server 316 of the access point 112
based on a standard HTTP protocol, such as HTTP 1.1 specification. The control agent
302 scans the web pages and obtains relevant information from the access point 112.
25 Any known data mining method and algorithm can be used for scanning and obtaining
the required information. The obtained information is then displayed on the GUI 304.
The control agent 302 is further adapted to send command to the access point 112 to
change the access point configurations and to control the network connecting through
the access point 112. The access point configurations include administrator and user
30 settings, IP address settings, encryption settings, firewall settings, etc. The control of
the network includes obtaining a list of devices connecting to the access point 112 for

monitoring and blocking/denying devices connecting to the access point. These controls can be performed through the GUI 304.

[0037] FIG. 4 illustrates a flow diagram showing the network monitoring process in accordance with one embodiment of the present invention. The flow diagram is illustrated in conjunction with the network management system of FIG. 3. The network monitoring step comprises establishing connection at step 410; logging in to the access point 112 at step 420; determining a device model at step 430; creating new model entry, if appropriate, at step 440; and managing a network access at step 450. In the step 410, the network management system is executed and establishing connection with the access point 112 at step 412. Once the connection is established, the control agent 302 opens a default home page at step 414. The default home page is stored in the HTTP server of the access point 112 used for accessing the access point 112. It is generally a HTTP page that manufacturer of the access point 112 provided to user to access configuration and monitor devices accessing the access point 112. The control agent 302 uses the HTTP protocol requests, such as the GET request under the HTTP 1.1 specification, for searching and opening the default home page assigned by the manufacturer. At the step 420, the user is required to log-in to the access point by providing an appropriate user name and password. A log-on window is shown to prompt for the user name and password at step 422. The access point 112 matches the input user name and password at step 424, and if matched, the user is allowed to access the access point 112.

[0038] Still referring to FIG. 4, once the user name and password are matched and the access to the access point 112 is allowed, the control agent 302 of the network management system determines the device model at the step 430. In step 430, the control agent 302 obtains a model and brand information of the access point 112 from the default home page at step 432. A signature-base (content-based) detection method can be used to obtain the model and brand information. The model and brand information is matched with a device library. The device library stores information of known access point models. The information includes pointers for scanning the

relevant data for network monitoring. The information for each device can be stored in the device library in a form of entry and the device library can be updated and expended as needed. When the model and brand information is matched with an entry of the device library at step 434, the control agent 302 initializes the entry's information for
5 extracting information from the access point at step 435. When the model and brand information does not match any entry of the device library, at step 434, or the control agent 302 is not able to find any model and brand information in the step 432, the control agent 302 creates a new entry in the device library at step 440. Once the new entry is created, the control agent 302 initializes the new entry's information for
10 extracting information from the access point at the step 435.

[0039] Still referring to FIG. 4, at step 450, the control agent 302 extracts the relevant information from the access point 112 based on the entry information, and the information is extracted continuously in a substantially real-time process. When
15 desires, user may control the devices connecting the access point 112 with the GUI 304.

[0040] FIG. 5 is a flow diagram illustrating a process for creating a new device entry for the device library in accordance with one embodiment of the present invention. The new device entry is created when the control agent 302 could not match
20 a model and brand entry with the model and brand information of the access point 112 at step 434 of FIG. 4. At step 500, the control agent 302 creates a new entry to be stored in the device library. At step 501, the control agent 302 scans for an URL link from the default html page. Keywords such as "http://" or the like are generally used for URL links within html pages. At step 502, the html page that the URL link linked is
25 opened. At step 503, the control agent 302 scans for keywords (including "http://") within the html page. Once the keywords are found, the locations of the keywords and URLs are recorded as part of the new device entry at step 504. The control agent 302 may scan the keywords using any known regular expression matching techniques. The control agent 302 then determines if more URL link is available for further scanning at
30 step 505. If more URL link is available, the control agent 302 loops back to step 501 to scan for all the available/possible URL links and record URL links for monitoring and

configuration. Upon completion of URL links scanning and new device entry creation, the control agent 302 performs the initialization of device entry as the step 435 of FIG. 4. In the loop from the step 501 to the step 505, the control agent 302 not only scans the URL link in the default html page, but all the URL links available in the html pages of the scanned URL links. The loop completes when all available/possible html pages within the access point 112 are scanned or required keywords and URLs are found.

[0041] FIG. 6 is a flow diagram illustrating a detailed process for network monitoring in step 450 of FIG. 4 in accordance with one embodiment of the present invention. After the control agent 302 initialized the device entry in step 435 of FIG. 4, the control agent 302 extracts all identity data of the devices connecting the access point 112 based on the device entry at step 602. At step 604, if the user of the network management system wants to block any devices connecting to the access point 112, the control agent 302 opens a specific html page for MAC address filtering provided by the access point 112. The MAC address of the selected device will be added to a MAC address field, and the access point 112 will start rejecting/blocking the corresponding device subsequently. At step 606, the control agent 302 loops back to step 602 recursively to updates the device connection status of the access point 112 at a predefined timing. The predefined timing of 5 seconds or less would be sufficient and can be considered a real-time scans.

[0042] During the process, the network management system acquires data from the access point by any web content mining methods known in the art.

[0043] In another embodiment, the network management system accesses a network access point 112 and operates based on scanning a hyper text language pages used for accessing the access point 112. The network management system provides a device library that stores information regarding access point of different models, the entries in the device library is then used to assist the network management system to determines the locations of the required information regarding the network connections' status. By that, the network can be monitored and controlled easily. In

the event that no record of an access point model is found, the network management system automatically search relevant hyper text language pages and relevant keywords regarding the field of interest from the hyper text language pages to generate a new device entry for the access point model in the device library.

5

[0044] Further, the network management system provides a recursive loop scanning process automatically. Upon each loop, there is a shot time delay, such as 5 seconds or less, before the next loop starts. Therefore, it is substantially a real-time monitoring in this specific application. As the network management system is able to
10 extract information from the access point of different models, user of the network management system requires to works in one application environment only, and understanding the operation and configuration of others access point of different models is not required.

15 **[0045]** It is a software agent that recited at network client devices, such as desktop computer or notebook computer. It provides alerts and identifications of the connected devices, whether trusted or un-trusted, at a given time. The user can use a single click to instruct a home wireless access point to block/reject any connected devices.

20

[0046] In accordance with another embodiment, the network management system can be configured to send alerts to the user of the network management system via any available communication means, such as E-mails and SMSs alerts. The network connections to the access point 112 are archived and logged for later usage.

25

[0047] In the above description, the network management system requires opening hyper text language pages for extracting data. It is possible the network management system opens the hyper text language pages and extracts data without actually showing the hyper text language pages. These operations are generally
30 performed at the background of the device hosting the network management system.

[0048] While specific embodiments have been described and illustrated, it is understood that many changes, modifications, variations and combinations thereof could be made to the present invention without departing from the scope of the invention.

Claims

1. A network management system for accessing an access point connecting at least one client device to form a network, the network management system comprising:
 - 5 a software agent for residing at the at least one client device, the software agent is operable to search for hyper text language pages stored in the access point and to extract relevant data regarding status of the network connections from the hyper text language pages; and
 - a graphical user interface for listing all client devices connecting the network
- 10 based on the extracted relevant data, the graphical user interface comprises controls for authorizing or blocking client devices connecting to network via the access point,
wherein the software agent updates the relevant data automatically at a predefined time.
- 15 2. The network management system according to claim 1, wherein the software agent is operable to search for hyper text language pages with regular expression of relevant keywords.
3. The network management system according to claim 1, wherein the software
- 20 agent is operable to search for hyper text language pages via requests under HTTP protocols.
4. The network management system according to claim 1, wherein the software agent is operable to extract the relevant data regarding status of the client devices with
- 25 regular expression of relevant keywords.
5. The network management system according to claim 1, wherein the software agent is operable to extract the relevant data regarding status of the client devices via requests under HTTP protocols.
- 30 6. The network management system according to claim 1, further comprising a device library for storing information regarding access point of different models.

7. The network management system according to claim 6, wherein the information regarding access point of different models includes pointers for appropriate hyper text language pages and the data regarding connection status.

5

8. The network management system according to claim 1, wherein the relevant data includes information regarding all the client devices connection status.

9. The network management system according to claim 1, wherein the relevant
10 data includes a model and brand of the access point.

10. The network management system according to claim 1, wherein the relevant data includes a MAC address, a IP address and a device name of the client devices.

15 11. The network management system according to claim 1, further comprising a user library includes information of the client devices authorized to connect to the network.

12. The method of accessing an access point connecting at least one client device to
20 form a network for managing the network connection, the method comprising:
searching for a hyper text language page for logging on to the access point;
logging on to the access point with user name and password;
searching for other hyper text language pages stored in the access point;
extracting relevant data regarding status of client devices connection from the
25 hyper text language pages;
listing all the client devices connecting the network on a graphical user interface
based on the extracted relevant data;
authorizing or blocking client devices connecting to the network via the access
point via the graphical user interface; and
30 updating the relevant data automatically at a predefined time.

13. The method according to claim 12, wherein the searching for the hyper text language pages is by way of using regular expression of relevant keywords.

14 The method according to claim 12, wherein the searching for the hyper text
5 language pages is based on requests under HTTP protocols.

15. The method according to claim 12, wherein extraction of the relevant data regarding status of the client devices is by way of regular expression of relevant keywords.

10

16. The method according to claim 12, wherein extraction of the data regarding status of the client devices is based on requests under HTTP protocols.

17. The method according to claim 12, further comprising storing information
15 regarding access point of different models.

18. The method according to claim 17, wherein the information regarding access point of different models includes pointers for appropriate hyper text language pages and the relevant data regarding connection status.

20

19. The method according to claim 12, wherein the relevant data includes information regarding all the client devices connection status.

20. The method according to claim 12, wherein the relevant data includes a model
25 and brand of the access point.

21. The method according to claim 12, wherein the relevant data includes a MAC address, a IP address and a device name of the client devices.

30 22. The method according to claim 12, further comprising adding a MAC address of a client device into a MAC address filtering list of the access point when the client device is to be blocked.