

METHOD AND SYSTEM FOR SECURING WIRELESS SYSTEMS AND DEVICES

Field of the Invention

5 **[0001]** The present invention relates to network and systems security. In particular, the invention relates to a system and method for wireless network security.

Background

10 **[0002]** As wireless services becoming more popular, there is a demand for one device that supports multiple wireless networks, such as wireless Personal Area Network (PAN), Wireless LAN (WLAN), Wireless Mesh, Wireless Metropolitan Area Network (WMAN), and etc, at the same time. For such device that supports multiple networks, the network securities become utmost important.

15

[0003] There are works and solutions proposed substantially to improve the security of WLAN starting from IEEE 802.11 standard Wired Equivalent Privacy (WEP) protocol, to 802.1X amendment to 802.1 specifications, to Temporal Key Integrity Protocol (TKIP) and Wi-Fi Protected Access (WPA/WPA2). Though security
20 standard such as WiFi Protected Access (WPA/WPA2) protocol work well for wireless devices supporting WLAN, it is not easy to address the security requirements of such devices and systems that support multiple wireless networks.

[0004] Wired Equivalency Privacy (WEP) is an encryption standard that was
25 used for wireless security. WEP comes in different key sizes. The common key lengths are currently 128- and 256-bit. The longer the better as it will increase the difficulty for crackers. However, as flaws were quickly discovered and exploited, it was shown that several open source utilities such as aircrack-ng, weplab, WEPCrack or airtsnort can be used to break in the WEP protected network by examining packets and
30 looking for patterns in the encryption. The major problem in WEP is that if packets on a network can be acquired, it is only a matter of time to crack the WEP encryption.

[0005] WEP is a shared key system, where the access point uses the same key as all clients devices and the clients devices also share the same key with each other. A hacker needs to only compromise the shared key from a single user, and the WEP protected network can be intruded. Further, the key for WEP protected network have to be either manually given to the end users for inputing to the connecting devices, or it has to be distributed to the connecting devices via other authentication method, which is cumbersome in most cases.

[0006] US publication no. 2006/0078124 entitled "System and Method for Providing WLAN Security through Synchronized Update and Rotation of WEP Keys" published on Apr. 13, 2006 discloses a system and method for updating WEP keys and rotate transmission key indices in a synchronized manner and on a frequent basis. The system and method uses WEP keys and it is catered for WLAN network only.

[0007] US publication no. 2007/0081672 entitled "Method to Enhance WLAN Security" published on Apr. 12, 2007 discloses a method for enhancing WLAN security by using an encryption algorithm in existing 802.11 standards. The encryption algorithm and it's keys are stored in an ID card. Similarly, the method is adapted for WLAN only as it uses WLAN network security parameters and keys for the encryption and decryption algorithm.

Summary

[0008] In accordance with one aspect of the present invention, there is provided a network security system comprises a key management system for generating keys for authentication, wherein the key comprises security parameters and supplementary parameters, wherein the supplementary parameters include a length of the key, a number of time that the security parameters are repeated within the length, and dummy characters.

30

[0009] In accordance with one embodiment, the security parameters may include any parameters in application, network and system level. The parameters in application level may include a login ID, a password and encryption/license keys. The

parameters in network and system level may include a WEP/WPA/WPA2 key, an encryption key, a service set identifier (SSID), a channel number, a frequency and a MAC address.

- 5 **[0010]** In accordance with another embodiment, parameters of the security parameters may be arranged in a pre-defined sequence.

[0011] In accordance with another embodiment, the network security system may further comprise a communication module for broadcasting the key to wireless
10 devices. The broadcasted key is synchronized between the wireless devices.

[0012] In yet another embodiment, the supplementary parameters may include a timestamp that define an expiry time for the key.

- 15 **[0013]** In yet another embodiment, the key management system may regenerate the keys for broadcasting to the wireless devices and synchronization between the wireless devices. It is possible that the key is regenerated on or before expiry of the key or when intruder is detected.

- 20 **[0014]** In accordance with another aspect, there is provided a method of securing a network comprises setting security parameters; setting supplementary parameters; and generating a key comprises the security parameters and supplementary parameters; wherein the supplementary parameters include a length of the key, a number of time that the security parameters are repeated within the length, and dummy
25 characters.

- [0015]** In accordance with one embodiment, the security parameters may include any parameters in application, network and system level. The parameters in application level may include a login ID, a password and encryption/license keys. The
30 parameters in network and system level may include a WEP/WPA/WPA2 key, an encryption key, a service set identifier (SSID), a channel number, a frequency and a MAC address.

[0016] In accordance with another embodiment, the security parameters may be arranged in a pre-defined sequence.

[0017] In accordance with another embodiment, the method may further
5 comprise broadcasting the key to wireless devices. The method may further comprise synchronizing the key between the wireless devices.

[0018] In yet another embodiment, the supplementary parameters may include a timestamp that define an expiry time for the key.

10

[0019] In yet another embodiment, the method may further comprise re-generating the key for broadcasting to the wireless devices and synchronization between the wireless devices. It is possible that the key is re-generated on or before expiry of the key or when intruder is detected.

15

Brief Description of the Drawings

[0020] This invention will be described by way of non-limiting embodiments of
20 the present invention, with reference to the accompanying drawings, in which:

[0021] FIG. 1 illustrates a diagram showing a wireless security system in accordance with an embodiment of the present invention; and

25 [0022] FIG. 2 exemplifies a key structure of a key in accordance with another embodiment of the present invention.

Detailed Description

[0023] 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 practised 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

[0024] FIG. 1 is a flow diagram illustrating a wireless security system **100** of a network in accordance with one embodiment of the present invention. The flow diagram shows a first wireless device **110** is communicating with a second device **120** wirelessly via a peer-to-peer connection. The connection is protected with the wireless security system **100** comprises a key management system **101** for managing encrypted keys for communication. The key management system **101** can be a standalone device or resided any wireless devices within the network. The wireless devices include access point, base stations, laptop computers, personal computers, PDAs, and other mobile wireless communication devices. The key management system **101** defines and distributes the encrypted keys to the wireless devices to protect the network communications. The key management system **101** is adapted to support multiple wireless networks such as WLAN, WPAN, WMAN and etc. The key management system **101** comprises a selection and sequencing module **102**, a random/user-defined entity generator **103**, a scheduling mechanism **104**, a database **105** and a communication module **106**. Briefly, the key management system **101** executes the selection and sequencing module **102** to set the security key parameters from the applications, network and system levels. The random/user-defined entity generator **103** allows the sequencing of the security key parameters be done by a random or user-defined process, or combinations of both. The random/user-defined entity generator **104** further acquires supplementary parameters for generating the key. The supplementary parameters can also be user-defined or randomly generated. Depending on the selected option (i.e. random or user-defined or combination), the scheduling mechanism **104** defined a key based on selected parameters and sequences. The key is

stored in the database **105** and is broadcasted to wireless devices (including the first wireless device **110** and the second wireless device **120**) of the network.

[0025] The selection and sequencing module **102** allows user to define the security parameters for the key. The security parameters are defined in applications, network and system levels. The application level's security parameters include a login ID, a password, encryption/license keys, and etc. The network and system levels' security parameters include a WEP/WPA/WPA2 key, an encryption key, a service set identifier (SSID), a channel number, a frequency, a MAC address, and etc. These security parameters can be selected based on the user-defined or random choice. The selected security parameters are sent to the entity generator **103**.

[0026] The entity generator **103** generates a set of entities that includes the security parameters and the supplementary parameters. In the entity generator **103**, sequences of the security parameters are defined to arrange the security parameters. The supplementary parameters include a count number, a length, dummy characters and a timestamp. The sequences of the security parameters and the supplementary parameters can be selected automatically in random or manually by user-defined manner or a combination of both. The supplementary parameters, together with the selected sequence of security parameters, are fed to the scheduling mechanism **104**.

[0027] The scheduling mechanism **104** defines a key in a function of the security parameters in sequence and the supplementary parameters with a timestamp, which can be denoted as equation (1),

$$\text{Key} = f(\text{security parameters in sequence, supplementary parameters}) + \text{timestamp} \quad (1)$$

[0028] In the scheduling mechanism **104**, all the parameters are defined as follows: the security parameters in application level are denoted as $A1, A2, \dots, An$, where $A1$ is an application security parameter 1; the security parameters in network level are denoted as $N1, N2, \dots, Nn$, where $N1$ is a network security parameter 1; and the security parameters of system level as $S1, S2, \dots, Sn$, where $S1$ is a system security parameter 1; the selected sequence of security parameters is denoted as Seq ; the count number is denoted as C ; the length is denoted as L ; the dummy characters are denoted

as D ; and the time stamp is denoted as T . Therefore, the key can be represented as equation (2),

$$Key = f(C, Seq, L, D) + T \quad (2)$$

5 **[0029]** The *Seq* includes any of the An , Nn , Sn and any of the combinations in any sequence defined by the user or randomly. Accordingly, the scheduling mechanism 104 generates the key that consists the *Seq* that is repeated for C number of time for as long as it is within the limit L . L must be large enough to cover at least one cycle of *Seq* repeating C time. The remaining within L , if any, is filled up with
10 randomly generated dummy characters, D . These dummy characters serve as noisy characters for deceiving intruders. The dummy characters can be in any length, depending on L . It is possible that L can be set sufficiently long to cater the dummy characters that occupy the majority of L to increase the challenge for hacking. The T is added to define an expiry time for all wireless systems and devices to get a new *Key*.

15

[0030] Once the *Key* is generated, it is stored in the database 105 and it is updated just before or on expiry of T .

[0031] The communication module 106 authenticates and sets-up
20 communication links with a normal communication channel establishment. Once the connection is established, the generated *Key* is sent to all authorized wireless devices which include the first wireless device 110 and the second wireless device 120. To maintain a secured transmission, the *Key* is re-generated and broadcasted to the authorized devices. When the new *Key* is generated and received by the devices,
25 devices re-configured themselves with this security parameters in the new *Key*, and upon which, the communication link is disconnected and re-connected again. That ensures a “private key” is used among the network without being hacked. A new key is generated when the T is expired, or when intrusion is detected. Once the re-configuration and re-connection are completed, the data transferring is resumed. The
30 purpose of the ever-changing keys is to raise the difficulties to obtain the *Key* without authorization, and even if a current *Key* is hacked by an intruder, it will not be long that the intruder needs to hack the new *Key* throughout the communication. Further, when the T is short, it may be more challenge to the intruders to hack into the network.

[0032] FIG. 2 exemplifies a customized key structure of a key 200 generated by the key management system 101. The key 200 is valid for 5 minutes and will be renewed thereafter for further communication between the wireless devices. During the valid period, the function 201 of the key 200 is repeated. The function 201 has a length of 10 seconds. Within the 10 seconds, the security parameters 202 which consists of $(A1, A2, N4, S2)$ are repeated for 5 times. Dummy characters 203 are randomly selected to fill up the function 201. Accordingly, the key 200 can be expressed in equation (2) as $Key = f(5, (A1, A2, N4, S2), 10, D) + 5$, where $C=5$, $L=10$ seconds, $T=5$ minutes and D is set random.

[0033] Referring back to FIG. 1, where a process of secure communication of two wireless devices 110 and 120 is shown. The process occurs in both wireless devices 110 and 120. In step 112, the communications module 106 establishes a wireless connection between the first wireless device 110 and the second wireless device 120 and initializes authentication. Once authenticated, the generated key is also downloaded to both wireless devices 110 and 120. The Key is stored until a new Key is received. The wireless devices 110 and 120 re-configure themselves based on the relevant security parameters information in the Key. Once the re-configuration is completed, the wireless devices 110 and 120 synchronizes with the key management system 101 through exchanging of handshaking signals before the communication link being set up again. Data transfer is taking place at the first instance. During the connection between the first wireless device 110 and the second wireless device 120, the key is used for authentication until the T , if any, expires. In normal data transfer stage, synchronization of new keys will be taking place among the key management system 101 and the wireless devices at the background. During data transfer, the wireless devices detect if there is any intruder in step 114. If intruder is detected, the wireless devices inform the key management system 101 to re-generate a new Key in step 115. In step 115, the devices are re-configured and reconnected again with the new Key. In step 116, the intruder's packets and activities are recorded and in step 117, important files or documents are deleted if require.

[0034] The present invention can be implemented on communication networks with different communication channels/protocols. For example, the key management system 101 is also applicable on a Peer to peer communications between different wireless devices. The wireless devices can also make use of the Key generated by the
5 key management system 101 to authenticate connections with other wireless devices.

[0035] The present invention provides a system and method of wireless security that supports multiple wireless networks. The common security parameters required by the respective wireless network and applications are grouped together and re-sequence
10 through a key management scheme. The present invention allows user to choose or define the combinations of the security parameters in applications, network, and systems level and sequences of the parameters.

[0036] An automated configuration system that includes an auto-
15 reconfiguration of the settings of one or all combination of either user selected or system defined security related parameters obtained from applications, network and systems levels so frequent that the intruder/hacker will not be able to use/hack into the system anymore within a reasonable amount of time.

[0037] Current technologies and implementations on network security focusing
20 on single wireless network device and system. The present invention provides a system and method integrating the security requirement/parameters based on application, network and system level that support multiple network protocols and systems. It is understood that the present invention is suitable not only for wireless network, but also
25 wired network.

[0038] The present invention is suitable to be implemented on a device supporting multiple network connection. It is especially useful for such device operating in ad-hoc networking or ad-hoc communication. For example, a device A
30 can have a secured key for a Wi-Fi connection with a device B, while at the same time, have another secured key for a 3.5G communication with device C, for which, data communication between devices B and C can be achieved through device A.

[0039] 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 security system comprising:
a key management system for generating keys for authentication, wherein the key comprises security parameters and supplementary parameters, wherein the
5 supplementary parameters include a length of the key, a number of time that the security parameters are repeated within the length, and dummy characters.
2. The network security system according to claim 1, wherein the security parameters include any parameters in application, network and system level.
10
3. The network security system according to claim 2, wherein the parameters in application level include a login ID, a password and encryption/license keys.
4. The network security system according to claim 2, wherein the parameters in
15 network and system level include a WEP/WPA/WPA2 key, an encryption key, a service set identifier (SSID), a channel number, a frequency and a MAC address.
5. The network security system according to claim 1, wherein parameters of the security parameters are arranged in a pre-defined sequence.
20
6. The network security system according to claim 1, further comprising a communication module for broadcasting the key to wireless devices.
7. The network security system according to claim 6, wherein the broadcasted key
25 is synchronized between the wireless devices.
8. The network security system according to claim 1, wherein the supplementary parameters include a timestamp that define an expiry time for the key.
- 30 9. The network security system according to claim 1, wherein the key management system re-generates the keys for broadcasting to the wireless devices and synchronization between the wireless devices.

10. The network security system according to claim 9, wherein the key is regenerated on or before expiry of the key.

11. The network security system according to claim 10, wherein the key is re-generated when intruder is detected.

12. A method of securing a network comprising:
setting security parameters;
setting supplementary parameters; and
generating a key comprises the security parameters and supplementary parameters;
wherein the supplementary parameters include a length of the key, a number of time that the security parameters are repeated within the length, and dummy characters.

13. The method according to claim 12, wherein the security parameters include any parameters in application, network and system level.

14. The method according to claim 13, wherein the parameters in application level include a login ID, a password and encryption/license keys.

15. The method according to claim 13, wherein the parameters in network and system level include a WEP/WPA/WPA2 key, an encryption key, a service set identifier (SSID), a channel number, a frequency and a MAC address.

16. The method according to claim 12, wherein parameters of the security parameters are arranged in a pre-defined sequence.

17. The method according to claim 12, further comprising broadcasting the key to wireless devices.

18. The method according to claim 17, further comprising synchronizing the key between the wireless devices.

19. The method according to claim 12, wherein the supplementary parameters include a timestamp that define an expiry time for the key.

20. The method according to claim 12, further comprising re-generating the key for
5 broadcasting to the wireless devices and synchronization between the wireless devices;

21. The method according to claim 19, wherein the key is re-generated on or before expiry of the key.

10 22. The method according to claim 20, wherein the key is re-generated when intruder is detected.