matter described herein exploits the hybrid of cellular and non-cellular networks to expand the coverage of cellular base stations. When a wireless device participates in a hybrid network, the subject method can configure the device's non-cellular interface to originate or relay a cellular communication via hopping on the non-cellular network. When connecting the device to a cellular network via hopping onto a non-cellular network, the device creates a secure tunnel between the device and the core of the cellular network. The secure tunnel can protect the data packets from being eavesdropped by another device during the communication path.

[005] In one aspect, described herein is a system that comprises: wirelessly connecting a wireless device to a cellular network by single-hopping or multi-hopping to a sink device in a non-cellular network, and establishing a security tunnel in the wireless communication between the wireless device and a first gateway, which is located in the cellular network. The establishment of the security tunnel is based on a security key assigned (non-limiting examples include: by the cellular network, by a cellular operator, by an end-user, and/or by a certificate authority) to the wireless device. The system further comprises transmitting data packets between the wireless device and the first gateway; the transmission comprises encrypting by the wireless device the data packets, sending by the wireless device the encrypted data packets over the security tunnel to the first gateway, receiving by the first gateway the encrypted data packets, decrypting by the first gateway the encrypted data packets, and updating a network connection table by the first gateway. In some embodiments, the system further comprises sending by the first gateway the decrypted data packets to the Internet. In some embodiments, the first gateway sends the decrypted data packets to a second gateway that in turn sends the decrypted data packets to the Internet.

[006] When data packets are sent from the Internet to the wireless device, the system comprises receiving the data packets by the first gateway. Alternatively, the data packets can be sent from the Internet to the second gateway that in turn sends the packets to the first gateway. The system further comprises transmitting data packets between the first gateway and the wireless device; the transmission comprises encrypting by the first gateway the data packets, sending by the first gateway the encrypted data packets over the security tunnel to the wireless device, receiving by the wireless device the encrypted data packets, and decrypting by the wireless device the encrypted data packets.

[007] The transmission of data packets between the wireless device and the first gateway and/or the second gateway involves billing the user of the wireless device the amount of data packets being sent. Using the hopping technologies, the sink/relaying devices allowing the wireless devices to hop onto the non-cellular network also transfer the same amount of data packets

sent/received by the wireless device. However, the courtesy of the sink/relaying devices should not be billed for the amount of data relayed. Therefore, the method further requests the first gateway and/or the second gateway to delete a billing record of the sink/relaying device.

BRIEF DESCRIPTION OF THE DRAWINGS

[008] **Figure 1** shows a non-limiting example of a hopping system; in this case, the sink device relays the cellular communication to the node devices that connect to the sink device by single-hopping or multi-hopping on the non-cellular network.

[009] **Figure 2** shows a non-limiting example of a multi-hop, hybrid network; in this case, the node device hops onto a sink device which in turn relays the signals to the cellular base station and one or more than one gateway in the cellular network.

[010] **Figure 3** shows a non-limiting example of a configuration of a hybrid network; in this case, the node device creates a security tunnel with the ePDG gateway.

[011] **Figure 4** shows a non-limiting example of a configuration of a hybrid network; in this case, the node device creates a security tunnel with the IP security gateway which is placed between the SGW and PGW gateways.

[012] **Figure 5** shows a non-limiting example of a configuration of a hybrid network; in this case, the node device creates a security tunnel with the IP security gateway which is placed before the SGW and PGW gateways.

[013] **Figure 6** shows a non-limiting example of a configuration of a hybrid network; in this case, the node device creates a security tunnel with the PGW gateway.

[014] **Figure 7**shows a non-limiting example of a configuration of an inter-RAT hybrid network; in this case, the node device operates on the HSPA protocol and the cellular network operates on the LTE protocol with SGW, PGW, and ePDG gateways.

[015] **Figure 8** shows a non-limiting example of a configuration of an inter-RAT hybrid network; in this case, the node device operates on the LTE protocol and the cellular network operates on the HSPA protocol with SGSN, PGW, and ePDG gateways.

[016] **Figure 9** shows a non-limiting example of a configuration of an inter-RAT hybrid network; in this case, the node device operates on the HSPA protocol and the cellular network operates on the LTE protocol with SGW, PGW, TTG, and GGSN gateways.

[017] **Figure 10** shows a non-limiting example of a configuration of an inter-RAT hybrid network; in this case, the node device operates on the LTE protocol and the cellular network

matter described herein exploits the hybrid of cellular and non-cellular networks to expand the coverage of cellular base stations. When a wireless device participates in a hybrid network, the subject method can configure the device's non-cellular interface to originate or relay a cellular communication via hopping on the non-cellular network. When connecting the device to a cellular network via hopping onto a non-cellular network, the device creates a secure tunnel between the device and the core of the cellular network. The secure tunnel can protect the data packets from being eavesdropped by another device during the communication path.

[005] In various aspects, described herein are systems and methods that comprise: wirelessly connecting a wireless device to a cellular network by single-hopping or multi-hopping to a sink device in a non-cellular network, and establishing a security tunnel in the wireless communication between the wireless device and a first gateway, which is located in the cellular network. The establishment of the security tunnel is based on a security key assigned (non-limiting examples include: by the cellular network, by a cellular operator, by an end-user, and/or by a certificate authority) to the wireless device. The system and methods further comprise transmitting data packets between the wireless device and the first gateway; the transmission comprises encrypting by the wireless device the data packets, sending by the wireless device the encrypted data packets over the security tunnel to the first gateway, receiving by the first gateway the encrypted data packets, decrypting by the first gateway the encrypted data packets, and updating a network connection table by the first gateway. In some embodiments, the system further comprises sending by the first gateway the decrypted data packets to the Internet. In some embodiments, the first gateway sends the decrypted data packets to a second gateway that in turn sends the decrypted data packets to the Internet.

[006] When data packets are sent from the Internet to the wireless device, the system comprises receiving the data packets by the first gateway. Alternatively, the data packets can be sent from the Internet to the second gateway that in turn sends the packets to the first gateway. The system and methods may further comprise transmitting data packets between the first gateway and the wireless device; the transmission comprises encrypting by the first gateway the data packets, sending by the first gateway the encrypted data packets over the security tunnel to the wireless device, receiving by the wireless device the encrypted data packets, and decrypting by the wireless device the encrypted data packets.

[007] The transmission of data packets between the wireless device and the first gateway and/or the second gateway involves billing the user of the wireless device the amount of data packets being sent. Using the hopping technologies, the sink/relaying devices allowing the wireless devices to hop onto the non-cellular network also transfer the same amount of data packets

sent/received by the wireless device. However, the courtesy of the sink/relaying devices should not be billed for the amount of data relayed. Therefore, the systems and methods further request the first gateway and/or the second gateway to delete a billing record of the sink/relaying device.

BRIEF DESCRIPTION OF THE DRAWINGS

[008] **Figure 1** shows a non-limiting example of a hopping system; in this case, the sink device relays the cellular communication to the node devices that connect to the sink device by single-hopping or multi-hopping on the non-cellular network.

[009] **Figure 2** shows a non-limiting example of a multi-hop, hybrid network; in this case, the node device hops onto a sink device which in turn relays the signals to the cellular base station and one or more than one gateway in the cellular network.

[010] **Figure 3** shows a non-limiting example of a configuration of a hybrid network; in this case, the node device creates a security tunnel with the ePDG gateway.

[011] **Figure 4** shows a non-limiting example of a configuration of a hybrid network; in this case, the node device creates a security tunnel with the IP security gateway which is placed between the SGW and PGW gateways.

[012] **Figure 5** shows a non-limiting example of a configuration of a hybrid network; in this case, the node device creates a security tunnel with the IP security gateway which is placed before the SGW and PGW gateways.

[013] **Figure 6** shows a non-limiting example of a configuration of a hybrid network; in this case, the node device creates a security tunnel with the PGW gateway.

[014] **Figure 7**shows a non-limiting example of a configuration of an inter-RAT hybrid network; in this case, the node device operates on the HSPA protocol and the cellular network operates on the LTE protocol with SGW, PGW, and ePDG gateways.

[015] **Figure 8** shows a non-limiting example of a configuration of an inter-RAT hybrid network; in this case, the node device operates on the LTE protocol and the cellular network operates on the HSPA protocol with SGSN, PGW, and ePDG gateways.

[016] **Figure 9** shows a non-limiting example of a configuration of an inter-RAT hybrid network; in this case, the node device operates on the HSPA protocol and the cellular network operates on the LTE protocol with SGW, PGW, TTG, and GGSN gateways.

[017] **Figure 10** shows a non-limiting example of a configuration of an inter-RAT hybrid network; in this case, the node device operates on the LTE protocol and the cellular network

CLAIMS

WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:
   a. connecting a wireless device to a cellular network by single-hopping or multi-hopping to a sink device in a non-cellular network; and
   b. establishing a security tunnel between the wireless device and a first gateway through the sink device.
2. The method of claim 1, wherein the first gateway comprises one or more of the following: an evolved packet data gateway, a packet data gateway, and an IPsec gateway.
3. The method of claim 1, wherein establishing the security tunnel is based on a key assigned to the wireless device by the cellular network.
4. The method of claim 1 further comprising:
   a. encrypting by the wireless device a first data packet, and generating an encrypted first data packet;
   b. sending by the wireless device the encrypted first data packet over the security tunnel to the first gateway;
   c. receiving by the first gateway the encrypted first data packet;
   d. decrypting by the first gateway the encrypted first data packet, and generating a decrypted first data packet; and
   e. updating a network connection table by the first gateway.
5. The method of claim 4, further comprising one or more of the following:
   a. modifying by the first gateway a source address of the decrypted first data packet,
   b. sending by the first gateway the decrypted first data packet to the Internet, and
   c. sending by the first gateway the decrypted first data packet to a second gateway.
6. The method of claim 5 further comprising one or more of the following:
   a. deleting by the first gateway a first billing record of the sink device,
   b. sending by the first gateway a request to the second gateway to delete a first billing record of the sink device,
   c. deep packet inspecting by the second gateway so that the second gateway does not create a first billing record of the sink device, and
   d. sending by the second gateway the decrypted first data packet to the Internet;

   wherein the second gateway comprises a packet data gateway
7. The method of claim 1, further comprising one or more of the following:
   a. receiving by the first gateway a second data packet from the Internet, and

b. receiving by the second gateway a second data packet from the Internet, and sending the second data packet to the first gateway.

8. The method of claim 7, further comprising modifying by the first gateway a destination address of the second data packet.

9. The method of claim 7, further comprising:

a. encrypting by the first gateway the second data packet, and generating an encrypted second data packet;

b. sending by the first gateway the encrypted second data packet over the security tunnel to the wireless device through the sink device;

c. receiving by the wireless device the encrypted second data packet; and

d. decrypting by the wireless device the encrypted second data packet and generating a decrypted second data packet.

10. The method of claim 9, further comprising one or more of the following:

a. deleting by the first gateway a second billing record of the sink device,

b. sending by the first gateway a request to the second gateway to delete the second billing record of the sink device, and

c. deep packet inspecting by the second gateway so that the second gateway does not create the second billing record of the sink device.

CLAIMS

WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:
    a. connecting a wireless device to a cellular network by single-hopping or multi-hopping to a sink device in a non-cellular network;
    b. establishing a security tunnel between the wireless device and a first gateway through the sink device;
    c. encrypting, by the wireless device, a first data packet, and generating an encrypted first data packet;
    d. sending, by the wireless device, the encrypted first data packet over the security tunnel to the first gateway;
    e. receiving, by the first gateway, the encrypted first data packet;
    f. decrypting, by the first gateway, the encrypted first data packet, and generating a decrypted first data packet;
    g. updating, by the first gateway, a network connection table;
    h. sending, by the first gateway, the decrypted first data packet to a second gateway; and
    i. sending, by the second gateway, the decrypted first data packet to the Internet.
2. The method of claim 1 further comprising one or more of the following:
    a. sending, by the first gateway, a request to the second gateway to delete a billing record of the sink device; and
    b. performing deep packet inspection, by the second gateway, and not creating the billing record of the sink device.
3. The method of claim 1, wherein (a) the first gateway comprises one or more of the following: an evolved packet data gateway and a tunnel termination gateway; and (b) the second gateway comprises one or more of the following: a packet data network gateway and a gateway GPRS support node.
4. The method of claim 1, wherein the establishing the security tunnel is based on a key assigned to the wireless device by the cellular network.
5. A computer-implemented method comprising:
    a. connecting a wireless device to a cellular network by single-hopping or multi-hopping to a sink device in a non-cellular network;
    b. establishing a security tunnel between the wireless device and a first gateway through the sink device;
    c. receiving, by a second gateway, a second data packet from the Internet;

d. sending, by the second gateway, the second data packet to the first gateway;

e. encrypting, by the first gateway, the second data packet, and generating an encrypted second data packet;

f. sending, by the first gateway, the encrypted second data packet over the security tunnel to the wireless device through the sink device;

g. receiving, by the wireless device, the encrypted second data packet; and

h. decrypting, by the wireless device, the encrypted second data packet and generating a decrypted second data packet.

6. The method of claim 5, further comprising one or more of the following:

a. sending, by the first gateway, a request to the second gateway to delete a billing record of the sink device; and

b. performing deep packet inspection, by the second gateway, and not creating the billing record of the sink device.

7. The method of claim 5, wherein (a) the first gateway comprises one or more of the following: an evolved packet data gateway and a tunnel termination gateway; and (b) the second gateway comprises one or more of the following: a packet data network gateway and a gateway GPRS support node.

8. The method of claim 5, wherein the establishing the security tunnel is based on a key assigned to the wireless device by the cellular network.

9. A system comprising:

a. a wireless device comprising a processor and a memory and configured to connect to a cellular network by single-hopping or multi-hopping to a sink device in a non-cellular network;

b. a first gateway configured to establish a security tunnel between the wireless device and the first gateway through the sink device; and

c. a second gateway;

wherein

the wireless device is further configured to (1) encrypt a first data packet and generate an encrypted first data packet; and (2) send the encrypted first data packet over the security tunnel to the first gateway; and

the first gateway is further configured to (1) receive the encrypted first data packet; (2) decrypt the encrypted first data packet and generate a decrypted first data packet; (3) update a network connection table; and (4) send the decrypted first data packet to the second gateway; and

the second gateway is configured to send the decrypted first data packet to the Internet.

10. The system of claim 9 further comprising one or more of the following:
    a. the first gateway is configured to send a request to the second gateway to delete a billing record of the sink device; and
    b. the second gateway is configured to perform deep packet inspection and does not create the billing record of the sink device.
11. The system of claim 9 wherein (a) the first gateway comprises one or more of the following: an evolved packet data gateway and a tunnel termination gateway; and (b) the second gateway comprises one or more of the following: a packet data network gateway and a gateway GPRS support node.
12. The system of claim 9, wherein the establishing the security tunnel is based on a key assigned to the wireless device by the cellular network.
13. A system comprising:
    a. a wireless device comprising a processor and a memory and configured to connect to a cellular network by single-hopping or multi-hopping to a sink device in a non-cellular network;
    b. a first gateway configured to establish a security tunnel between the wireless device and the first gateway through the sink device; and
    c. a second gateway;

    wherein

    the second gateway is configured to (1) receive a second data packet from the Internet; and (2) send the second data packet to the first gateway;

    the first gateway is further configured to (1) encrypt the second data packet and generate an encrypted second data packet; and (2) send the encrypted second data packet over the security tunnel to the wireless device through the sink device;

    the wireless device is further configured to (1) receive the encrypted second data packet; and (2) decrypt the encrypted second data packet and generate a decrypted second data packet.
14. The system of claim 13 further comprising one or more of the following:
    a. the first gateway is configured to send a request to the second gateway to delete a billing record of the sink device; and
    b. the second gateway is configured to perform deep packet inspection and does not create the billing record of the sink device.
15. The system of claim 13, wherein (a) the first gateway comprises one or more of the following: an evolved packet data gateway and a tunnel termination gateway; (b) the second gateway comprises one or more of the following: a packet data network gateway

and a gateway GPRS support node; and (c) the establishing the security tunnel is based on a key assigned to the wireless device by the cellular network.