(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 January 2008 (31.01.2008)

PCT

(10) International Publication Number
WO 2008/012759 A2

(51) International Patent Classification:
H04L 12/44 (2006.01)

(21) International Application Number:
PCT/IB2007/052925

(22) International Filing Date: 23 July 2007 (23.07.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
200610107903.5 24 July 2006 (24.07.2006) CN

(71) Applicant *(for all designated States except US)*: **UTSTARCOM TELECOM CO., INC.** [CN/CN]; No. 368 LiuHe Road, Bingjiang, Hangshou Zhejiang 310053 (CN).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LI, Dong** [CN/CN]; 3rd Floor Legend Building, High-Tech Industry Park, Nanshen Shenzhen Guangdong 518057 (CN). **LI, Desheng** [CN/CN]; 3rd Floor Legen Building, High-Tech Industry Park, Nanshen Shenzhen Guangdong 518057 (CN). **LI, Hongmin** [CN/CN]; 3rd Floor Legend Building, High-Tech Industry Park, Nanshen Shenzhen Guangdong 518057 (CN).

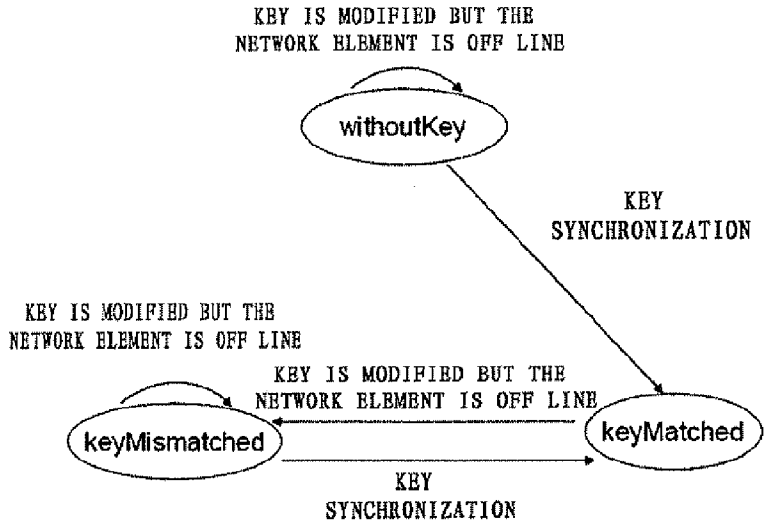
(74) Agents: **MACKINNON, Charles** et al.; 3800 Golf Road, Suite 220, Rolling Meadows, IL 60008 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: A NETWORK MANAGEMENT METHOD BASED ON SNMP



(57) Abstract: The object of the present invention is to provide a network management method based on SNMP with high security, comprising the following steps: (a) initiating and initializing the NMS; (b) the NMS detecting communication state and key state of the network element to determine whether or not a key synchronization with the network element is required; (c) the NMS generating a SNMP Get request for querying the current information on the network element and sending it to the network element that returns a SNMP response containing the queried current information on the network element; (d) the NMS generating a SNMP Set request for controlling/configuring the network element, encrypting and sending the generated SNMP Set request to the network element that returns a SNMP response containing a control/configuration result. Therefore, by encrypting the SNMP request, the managed network can be protected from being attacked via the SNMP Set request, thereby ensuring sufficient security.

WO 2008/012759 A2

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A Network Management Method Based on SNMP

FIELD OF THE INVENTION

The present invention relates to security management of a communication network, and more particularly, to a network management method based on SNMP (Simple Network Management Protocol) in the communication network management.

BACKGROUND OF THE INVENTION

Fig.1 is a schematic diagram showing a network management structure. In Fig.1, network management is performed based on SNMP between a NMS and a managed network (network element), wherein NMS (Network Management System) comprises a NMS application layer and a NMS communication layer. Further, SNMP is a management protocol widely used in the telecommunication network management filed, and SNMP provides a method of collecting network management information from network devices and controlling/configuring network configuration, and provides for the devices a method of reporting to the NMS of problems and errors.

In general, the process of performing telecommunication network management between the NMS and the managed network (network element) is as follows: the NMS application layer sends a query or control/configuration request to the NMS communication layer; the NMS communication layer converts this request into a SNMP Get/Set request and interacts with a managed telecommunication device. If the managed telecommunication network is in fault or abnormal, the telecommunication device will send a SNMP trap to the NMS.

At present, many telecommunication devices are directly deployed on the Internet, thus, how to securely manage them and how to protect these

devices from being attacked via the SNMP request, particularly, the SNMP Set request, is crucial.

If a hacker knows a MIB definition of the managed telecommunication device, he/she can easily control and/or re-configure the telecommunication device by simulating or tampering the SNMP Set request so as to reach the purpose of attacking. These control/configuration operations may be: (1) reboot or reset of software and hardware; (2) power off or operation stop of the hardware; (3) manual switch of systems; (4) modification of cross connection; and (5) reconfiguration of service-related parameters. All these operations may influence or interrupt telecommunication services, thereby bringing a huge calamity to the telecommunication network.

The main way to solve this problem is to use SNMP V3, i.e. using the security mechanism supported by SNMP V3 to protect the managed telecommunication device from being attacked. However, the use of the SNMP V3 has the following defects: (1) the SNMP V3 is too complex to be a "simple" network management protocol, thereby complicating its implementation; and (2) many existing telecommunication devices and SNMP developing tools do not support the SNMP V3.

SUMMARY OF THE INVENTION

In view of the above defects, an object of the present invention is to provide a network management method based on SNMP with high security.

The present invention provides a network management method that performs network management between NMS and a plurality of network elements based on SNMP, characterized in that said method comprises the following steps:

(a) initiating and initializing the NMS;

(b) the NMS detecting communication state and key state of a network

element to determine whether or not a key synchronization with the network element is required;

(c) the NMS generating a SNMP Get request for querying the current information on the network element and sending it to the network element that returns a SNMP response containing the queried current information on the network element; and

(d) the NMS generating a SNMP Set request for controlling/configuring the network element, encrypting and sending the generated SNMP Set request to the network element that returns a SNMP response containing a control/configuration result.

The above said step (a) comprises the following steps:

(a1) initiating the NMS; and

(a2) the NMS reading the key from a key file and assigning the key to a latestKey for recording a latest key in the NMS.

The above said step (b) comprises:

a communication state detecting step and a key state detecting step,

wherein the key state of the network element is defined to any one of withoutKey, keyMatched, and keyMismatched,

and wherein in the key state detecting step, if the key state of the network element is detected to be the KeyMatched, it indicates that the key of the network element matches with the NMS; if the key state of the network element is detected to be the withoutKey, the NMS delivering the key file to the network element by means of SFTP mdoe, modifying the key state of the network element to KeyMatched and setting the currently used key to the latestKey; if the key state of the network element is detected to be the keyMismatched, the NMS delivering the key file to the network element by means of SFTP mode, informing the network element of key update via the encrypted SNMP Set request, modifying the key state of the network element

to the KeyMatched and setting the key currently used by the network element to the latestKey.

The above said step (c) comprises the following steps: (c1) the NMS judging whether or not the network element is on line; (c2) if the network element is on line, the NMS generating the SNMP Get request; (c3) the NMS sending the generated SNMP Get request to the network element; and (c4) the NMS receiving the SNMP response sent from the network element.

The above said step (d) comprises the following steps:

(d1) the NMS judging whether or not the network element is on line;

(d2) if the network element is on line, the NMS checking the key state of the network element;

(d3) the NMS generating the SNMP request from the control/configuration request;

(d4) the NMS encrypting the SNMP Get request with the key currently used by the network element and sending the encrypted SNMP Set request to the network element; and

(d5) the NMS obtaining the SNMP response containing the control/configuration result from the network element.

In the above said step (d2), if the key state of the network element is the KeyMatched, it indicates that the key of network element matches with the NMS; if the key state of the network element is the withoutKey, the NMS delivering the key file to the network element by means of SFTP mode, modifying the key state of the network element to the KeyMatched and setting the currently used key to the latestKey; if the key state of the network element is the keyMismatched, the NMS delivering the key file to the network element by means of SFTP mode, informing the network element of key update via the encrypted SNMP Set request, modifying the key state of the network element to the KeyMatched and setting the key currently used by

the network element to the latestKey.

In case of a network fault, said method comprises the following steps :

(I) the network element sending a SNMP trap to the NMS;

(II) the NMS determining the type of the trap;

(III) if the trap is NERestart, the NMS checking the key state of the network element and performing key synchronization when necessary: if the key state of the network element is the keyMatched, it indicates that the key of the network element matches with the NMS; if the key state of the network element is the withoutKey, the NMS delivering the key file to the network element by means of SFTP mode, modifying the key state of the network element to the keyMatched and setting the currently used key to the latestKey; if the key state of the network element is the keyMismatched, the NMS delivering the key file to the network element by means of SFTP mode, informing the network element of key update via the encrypted SNMP Set request, modifying the key state of the network element to the keyMatched, and setting the key currently used by the network element to the latestKey.

(IV) if the trap is NERequestKeyInfo, the NMS delivering the key file to the network element by means of SFTP mode, and the NMS modifying the key state of the network element from the withoutKey to the keyMatched, and setting the key currently used by the network element to the latestKey.

Further, in the case of creating a new network element in the NMS, said method comprises the following steps :

the NMS modifying the key state of the network element to the withoutKey;

the NMS detecting whether or not the network element is on line; if the network element is on line, the NMS delivering the key file to the network element by means of SFTP mode, modifying the key state of the network element from the withoutKey to the keyMatched, and setting the key

currently used by the network element to the latestKey.

Further, in the case of modifying the key at the network element side from the NMS side, said method comprises the following steps:

(I) the NMS generating a new key and assigning it to the latestKey;

(II) the NMS generating a new key file from the newly generated key;

(III) the NMS communicatign with the network element to update the key file and the key at the network element side.

In the above said step (III), if the network element is on line, the NMS delivering the key file to the network element by means of SFTP mode, informing the network element of the key update via the encrypted SNMP Set request, modifying the key state of the network element to the keyMatched, and setting the key currently used by the network element to latestKey; if the network element is off line and its key state is the keyMatched, the NMS modifying its key state to the keyMismatched.

The SNMP Set request is encrypted with an old key in the network element.

As described above, by encrypting the SNMP Set request, the managed network can be protected from being attacked via the SNMP Set request, thereby efficiently ensuring security.

As described above, the key is delivered to the network element side by means of SFTP (Secured FTP) mode, wherein SFTP is based on SSH (Secure Shell) and encrypts all the transmitted data by use of SSH, thus the attacking manner like "go between" cannot be achieved and DNS and IP cheat can be prevented. In addition, since the data transmitted in SSH is compressed, the transmission speed can be accelerated. It follows that, in the present invention, by delivering the key by means of SFTP mode, the security in the course of delivering the key can be ensured.

Further, as described above, in the present invention, in order to ensure

security, the operator can modifying the key periodically, thereby protecting the SNMP Set request from being easily simulated or tampered.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig.1 is a schematic diagram showing a network management structure;

Fig.2 is a state diagram showing a key state at the network element side;

Fig.3 is a flowchart showing processing of a SNMP Get request and a SNMP response in the NMS;

Fig4 is a flowchart showing processing of a SNMP Get request in the NMS;

Fig.5 is a flowchart showing processing of a SNMP Trap in the NMS;

Fig.6 is a flowchart showing processing of creating a new network element in the NMS; and

Fig.7 is a flowchart showing processing of modifying the key in the NMS.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The network management method based on SNMP of the present invention will be described below with reference to Figs.2-7.

In the network management method based on SNMP of the present invention, network management is performed between the NMS and the network elements based on SNMP, and main flow of the method comprises the following steps:

initiating and initializing the NMS;

the NMS detecting communication state and key state of the network element to determine whether or not a key synchronization with the network element is required;

the NMS generating a SNMP Get request for querying the current

information on the network element and sending it to the network element that returns a SNMP response containing the queried current information on the network element;

the NMS generating a SNMP Set request for controlling/configuring the network element, encrypting and sending the generated SNMP Set request to the network element that returns a SNMP response containing a control/configuration result.

As regards the key state of the network element, as shown in Fig.2, we define three states: withoutKey, keyMatched, and keyMismatched, wherein the withouKey indicates that the network element is in its initial state (without key), and since an operator has created it in the NMS, it is off line all the time (e.g. the network element is not powered on or cannot communicate with the NMS due to the network), thus the NMS cannot deliver the key to it (or synchronize with it); the keyMismatched indicates that the key of the network element does not match with the NMS; and the keyMatched indicates that the key has been successfully delivered to the network element side (or synchronized with it) and matches with the NMS.

In order to manage the key state of each network element and the currently used key, we define a data structure as follows:

structure {

int keyState; the key state of the network element which takes a value of withoutKey, keyMatched, or keyMismatched

string currentKey; recording the key currently used by the network element

}

A global variable latestKey is also introduced here to record the latest key in the NMS.

The process of initiating and initializing the NMS as in the above step

(a)specifically comprises the following steps: (a1) initiating the NMS; (a2) the NMS reading the key from a key file and assigns the key to the latestKey; (a3) the NMS sending a SNMP request to the network element and processing a SNMP response returned from the network element, or receiving and processing a trap (the trap will be described below) sent from the network element, or providing the user with an operating interface.

As regards the initialization, generally, there is a default key file in a NMS initial package. If the operator does not modify the key after deploying the NMS, the NMS will use this default key to communicate with all the managed network elements, in which case, what is assigned to the latestKey when initializing the NMS is the default key; otherwise, if the operator modifies the key after deploying the NMS, what is assigned to the latestKey when initializing the NMS is the modified key.

In addition, the above-mentioned "key file" is stored at any location accessible by the NMS, and content of the key file is pure key information (KEY).

Further, the above step (b) comprises two steps: the NMS detecting the communication state and the key state of the network element.

Firstly, in order to facilitate the NMS to deliver the key to the network element (or synchronize with it), the NMS needs to detect whether or not the communication state of each network element is recovered. In the present invention, the following two ways may used to detect it: (1) the NMS polls each network element periodically to detect whether or not they are on line; (2) the network element sends a trap NERestart (the trap NERestart will be described below) to the NMS after being initiated or rebooted successfully, to inform the NMS that the network element has been on line.

Secondly, when the NMS detects that the network element has recovered its communication or the NMS needs to send a SNMP request to a network

element, the NMS needs to detect the key state of the network element and performs "key synchronization" with the network element when necessary. This processing flow comprises: (1) the NMS detects the key state of the network element to determine whether the key is delivered to the network element or whether the key is modified; (2) if the key state of the network element is KeyMatched, it indicates that the key is matched; if the key state of the network element is withoutKey, the NMS will deliver the key file to the network element by means of SFTP (secured FTP: secured file transfer protocol) mode, modify the key state of the network element to KeyMatched and set the currently used key to latestKey; if the key state of the network element is keyMismatched, the NMS will deliver the key file to the network element by means of SFTP mode, inform the network element of key update via the SNMP Set request, modify the key state of the network element to KeyMatched and set the key currently used by the network element to the latestKey.

Fig.3 is a flowchart showing processing of a SNMP Get request and a SNMP response in the NMS. The NMS uses the SNMP Get request to communicate with the network element to obtain the current information on the network element.The flow of processing the SNMP Get request and the SNMP response is shown in Fig.3: (1) the NMS application layer sends a query request to the NMS communication layer; (2) the NMS communication layer checks whether or not the network element to be communicated with is on line, if the network element is off line, the NMS communication layer returns "failure" to the NMS application layer; (3) if the network element is on line, the NMS communication layer generates the SNMP Get request from the query request sent from the NMS application layer, the NMS communication layer sends the generated SNMP Get to the network element, the NMS communication layer receives the SNMP response sent from the

network element and returns the result queried from the network element to the NMS application layer.In such a way, communicating with the network element is performed by sending the SNMP Get request from the NMS side to the network element, thus, the current information on the network element can be obtained at the NMS side.

Fig.4 is a flowchart showing processing of a SNMP Set request in the NMS. The SNMP Set request is a request to perform a control/configuration operation on the network element. In order to improve security of network management in the present invention, the SNMP Set request is encrypted. A specific flow for processing the SNMP Set request is shown in Fig.4: (1) the NMS application layer sends a network element control/configuration request to the NMS communication layer; (2) the NMS communication layer detects whether or not the network element to be communicated with is on line; (3) if the network element is off line, the NMS communication layer returns "failure" to the NMS application layer; if the network element is on line, the processing flow is as follows:

(a) the NMS communication layer checks the key state of the network element; if its key state is withoutKey or keyMismatched, the NMS needs to perform "key synchronization" with the network element (the flowchart of the "key synchronization" sees the above);

(b) the NMS communication layer generates the SNMP Set request based on the control/configuration request from the NMS application layer;

(c) the NMS communication layer uses the key currently used by the network element to encrypt the SNMP Set request;

(d) the NMS communication layer sends the encrypted SNMP Set request to the network element;

(e) the NMS communication layer receives a SNMP response sent from the network element;

(f) the NMS communication layer returns the control/configuration result returned by the network element to the NMS application layer.

The method for encrypting the SNMP Set request is not limited to a particular encrypting algorithm, and any encrypting algorithm is possible, e.g. AES (Advanced Encryption Standard), DES (Data Encryption Standard), RSA (Rivest Shamir Adelman).

If the managed network element is in fault or abnormal, the network element will send a SNMP trap to the NMS. Fig.5 is a flowchart showing processing of the SNMP Trap in the NMS. As shown in Fig.5, the processing flow of the SNMP Trap is as follows: if the network element is in fault, the following steps take place:

(1) the network element sends the SNMP trap to the NMS;

(2) the NMS determines the type of the trap;

(3) if the trap is NERestart, the NMS checks the key state of the network element and performs key synchronization when necessary. That is, if the key state of the network element is keyMatched, it indicates that the key of the network element matches with the NMS; if the key state of the network element is withoutKey, the NMS delivers the key file to the network element by means of SFTP mode, modifies the key state of the network element to keyMatched and sets the currently used key to latestKey; if the key state of the network element is keyMismatched, the NMS delivers the key file to the network element by means of SFTP mode, informs the network element of key update via the encrypted SNMP Set request, modifies the key state of the network element to keyMatched, and sets the key currently used by the network element to latestKey.

(4) if the trap is NERequestKeyInfo, the NMS delivers the key file to the network element by means of SFTP mode, and the NMS modifies the

key state of the network element from withoutKey to keyMatched, and sets the key currently used by the network element to latestKey.

Other types of trap are processed the same as in the prior art.

When the operator creates a new network element, the key file is required to be delivered from the NMS to the newly created network element. Fig.6 is a flowchart for processing of creating a new network element in the NMS. As shown in Fig.6, the processing flow for creating a new network element in the NMS is as follows:

(1) the user creates a new network element in the NMS;

(2) the NMS modifies the key state of the network element to withoutKey;

(3) the NMS detects whether or not the network element is on line;

(4) if the network element is on line, the NMS delivers the key file to the network element by means of SFTP mode, modifies the key state of the network element from withoutKey to keyMatched, and sets the key currently used by the network element to latestKey.

In order to further ensure security of the network system, the operator can modify the key periodically so as to reliably protect the SNMP Set request from being tampered or simulated.

Fig.7 is a flowchart showing processing of modifying the key in the NMS. As shown in Fig.7, the processing flowchart for modifying the key is as follows:

(1) the operator uses a NMS client to trigger the NMS to modify the key;

(2) the NMS generates a new key and assigns it to the latestKey;

(3) the NMS generates a new key file according to the newly generated key;

(4) the NMS attempts to communicate with each managed network

element to update the key file and the key at the network element side.

For each network element, the flow for updating the key file and the key is as follows: (a) if the network element is on line, the NMS delivers the key file to the network element by means of SFTP mode, informs the network element of the key update via the SNMP Set request. The SNMP Set request is encrypted with an old key recorded in a currentKey of the network element, modifies the key state of the network element to keyMatched, and sets the key currently used by the network element to latestKey; (b) if the network element is off line and its key state is keyMatched, the NMS modifies its key state to keyMismatched; otherwise, the NMS does nothing.

Since encryption and decryption correspond to each other, after the encrypting mechanism is added as described above, the network element agent (NMS Agent) processing flow needs to be adaptively amended as follows:

(1) the network element agent is initiated and initialized;

(2) the network element agent sends a trap NERestart to the NMS;

(3) the network element agent identifies its state to "without key";

(4) the network element agent goes to the following loop: (a) if the state of the network element agent is "without key", it checks periodically whether or not the NMS delivers the key file; if the key file is locally available, it reads the key from the key file and identifies its state to "with key"; (b) if the agent at the network element side has a state of "without key", it will periodically transmit a trap NERequestKeyInfor to request the NMS for the key; (c) receives and processes the SNMP request from the NMS: (c1) if the PDU (Protocol Data Unit) is a SNMP Get request, since both the SNMP Get request and the SNMP response are not encrypted, they are processed the same way as in the prior art without introducing the encryption mechanism; (c2) if the PDU is an encrypted SNMP Set request, and the network element

agent has a state of "with key", it will decrypt the received SNMP PDU and check whether the SNMP request is a request for the NMS to trigger it to modify the key; if the SNMP request is the request for triggering it to modify the key, the network element agent will read the latest key from the key file delivered by the NMS; otherwise, the SNMP Set request is processed the same way as in the prior art without introducing the encryption mechanism; if the state of the network element agent is "without key", it will discard the received SNMP Set request and do nothing, because it has no key to decrypt the SNMP PDU; (d) the network element agent manages all the local managed resources, and if there are faults or abnormities, it will send the SNMP trap to the NMS, and the processing is the same as in the prior art without introducing the encrypting mechanism.

As described above, by encrypting the SNMP Set request, the managed network can be protected from being attacked via the SNMP Set request, thereby efficiently ensuring security.

Further, as described above, the key is delivered to the network element side by means of SFTP mode, thus, the security in the course of delivering the key can be ensured.

Moreover, as described above, in the present invention, the operator can further protect the SNMP Set request from being easily simulated or tampered by modifying the key periodically, thereby further improving security.

The specific embodiments of the invention have been described above with reference to the accompanying drawings. However, those skilled in the art would appreciate that, various modifications to the embodiments could be made without departing from the spirit of the invention and the scope defined by the appended claims. Therefore, the specific embodiments of the invention described with reference to the accompanying drawings shall not be regarded as limit to the present invention.

Claims

1. A network management method based on SNMP that performs network management between NMS and a plurality of network elements based on SNMP, characterized in that said method comprises the following steps:

(a) initiating and initializing the NMS;

(b) the NMS detecting communication state and key state of a network element to determine whether or not a key synchronization with the network element is required;

(c) the NMS generating a SNMP Get request for querying the current information on the network element and sending it to the network element that returns a SNMP response containing the queried current information on the network element; and

(d) the NMS generating a SNMP Set request for controlling/configuring the network element, encrypting and sending the generated SNMP Set request to the network element that returns a SNMP response containing a control/configuration result.

2. A network management method based on SNMP according to Claim 1, characterized in that the step (a) comprises the following steps:

(a1) initiating the NMS; and

(a2) the NMS reading the key from a key file and assigning the key to a latestKey for recording a latest key in the NMS.

3. A network management method based on SNMP according to Claim 1, characterized in that the step (b) comprises:

a communication state detecting step and a key state detecting step,

wherein the key state of the network element is defined to any one of withoutKey, keyMatched, and keyMismatched,

and wherein in the key state detecting step, if the key state of the network element is detected to be the KeyMatched, it indicates that the key of the network element matches with the NMS; if the key state of the network element is detected to be the withoutKey, the NMS delivering the key file to the network element by means of SFTP mdoe, modifying the key state of the network element to KeyMatched and setting the currently used key to the latestKey; if the key state of the network element is detected to be the keyMismatched, the NMS delivering the key file to the network element by means of SFTP mode, informing the network element of key update via the encrypted SNMP Set request, modifying the key state of the network element to the KeyMatched and setting the key currently used by the network element to the latestKey.

4. A network management method based on SNMP according to Claim 3, characterized in that the SNMP Set request is encrypted with an old key in the network element.

5. A network management method based on SNMP according to Claim 1, characterized in that the step (c) comprises the following steps: (c1) the NMS judging whether or not the network element is on line; (c2) if the network element is on line, the NMS generating the SNMP Get request; (c3) the NMS sending the generated SNMP Get request to the network element; and (c4) the NMS receiving the SNMP response sent from the network element.

6. A network management method based on SNMP according to Claim 1, characterized in that the step (d) comprises the following steps:

(d1) the NMS judging whether or not the network element is on line;

(d2) if the network element is on line, the NMS checking the key state of the network element;

(d3) the NMS generating the SNMP request from the control/configuration request;

(d4) the NMS encrypting the SNMP Get request with the key currently used by the network element and sending the encrypted SNMP Set request to the network element; and

(d5) the NMS obtaining the SNMP response containing the control/configuration result from the network element.

7. A network management method based on SNMP according to Claim 6, characterized in that in the step (d2), if the key state of the network element is the KeyMatched, it indicates that the key of network element matches with the NMS; if the key state of the network element is the withoutKey, the NMS delivering the key file to the network element by means of SFTP mode, modifying the key state of the network element to the KeyMatched and setting the currently used key to the latestKey; if the key state of the network element is the keyMismatched, the NMS delivering the key file to the network element by means of SFTP mode, informing the network element of key update via the encrypted SNMP Set request, modifying the key state of the network element to the KeyMatched and setting the key currently used by the network element to the latestKey.

8. A network management method based on SNMP according to Claim 1, characterized in that in case of a network fault, said method comprises the following steps :

(I) the network element sending a SNMP trap to the NMS;

(II) the NMS determining the type of the trap;

(III) if the trap is NERestart, the NMS checking the key state of the network element and performing key synchronization when necessary: if the key state of the network element is the keyMatched, it indicates that the key of the network element matches with the NMS; if the key state of the network element is the withoutKey, the NMS delivering the key file to the network element by means of SFTP mode, modifying the key state of the network element to the keyMatched and setting the currently used key to the latestKey; if the key state of the network element is the keyMismatched, the NMS delivering the key file to the network element by means of SFTP mode, informing the network element of key update via the encrypted SNMP Set request, modifying the key state of the network element to the keyMatched, and setting the key currently used by the network element to the latestKey.

(IV) if the trap is NERequestKeyInfo, the NMS delivering the key file to the network element by means of SFTP mode, and the NMS modifying the key state of the network element from the withoutKey to the keyMatched, and setting the key currently used by the network element to the latestKey.

9. A network management method based on SNMP according to Claim 1, characterized in that in the case of creating a new network element in the NMS, said method comprises the following steps :

the NMS modifying the key state of the network element to the withoutKey;

the NMS detecting whether or not the network element is on line; if the network element is on line, the NMS delivering the key file to the network element by means of SFTP mode, modifying the key state of the network element from the withoutKey to the keyMatched, and setting the key currently used by the network element to the latestKey.

10. A network management method based on SNMP according to Claim 1, characterized in that in the case of modifying the key at the network element side from the NMS side, said method comprises the following steps :

(I) the NMS generating a new key and assigning it to the latestKey;

(II) the NMS generating a new key file from the newly generated key;

(III) the NMS communicatign with the network element to update the key file and the key at the network element side.

11. A network management method based on SNMP according to Claim 10, characterized in that in the step (III), if the network element is on line, the NMS delivering the key file to the network element by means of SFTP mode, informing the network element of the key update via the encrypted SNMP Set request, modifying the key state of the network element to the keyMatched, and setting the key currently used by the network element to latestKey; if the network element is off line and its key state is the keyMatched, the NMS modifying its key state to the keyMismatched.

12. A network management method based on SNMP according to Claim 11, characterized in that the SNMP Set request is encrypted with an old key in the network element.

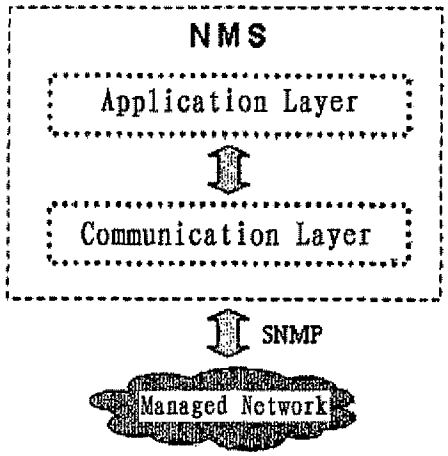

NMS
Application Layer
Communication Layer
SNMP
Managed Network

Fig. 1

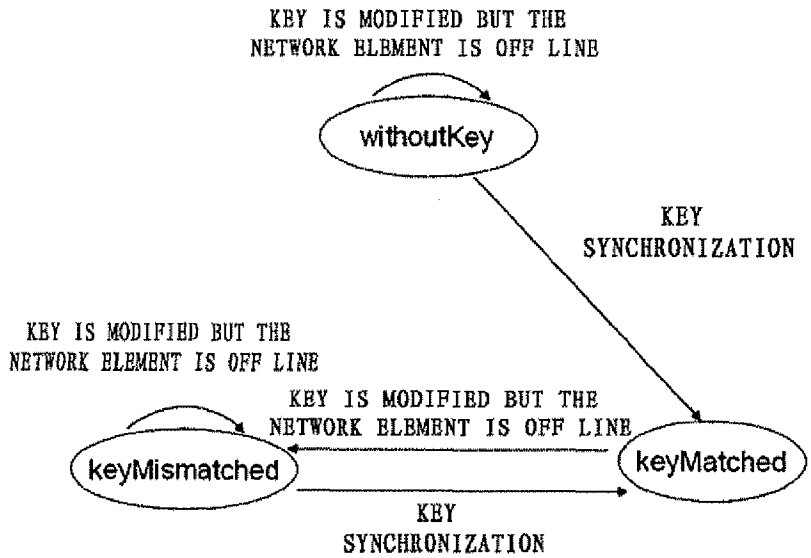

KEY IS MODIFIED BUT THE NETWORK ELEMENT IS OFF LINE
withoutKey
KEY SYNCHRONIZATION
KEY IS MODIFIED BUT THE NETWORK ELEMENT IS OFF LINE
KEY IS MODIFIED BUT THE NETWORK ELEMENT IS OFF LINE
keyMismatched
keyMatched
KEY SYNCHRONIZATION

Fig. 2

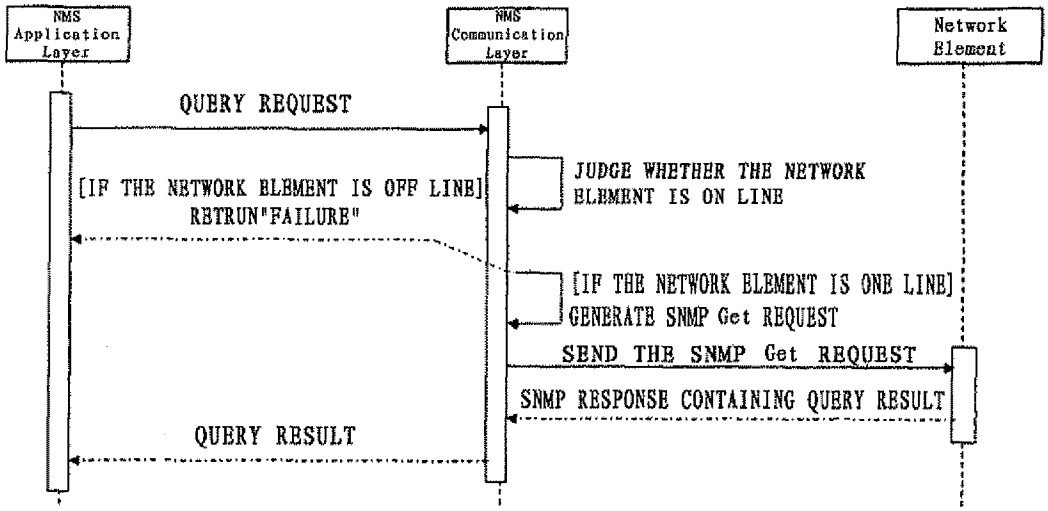

NMS Application Layer
NMS Communication Layer
Network Element
QUERY REQUEST
JUDGE WHETHER THE NETWORK ELEMENT IS ON LINE
[IF THE NETWORK ELEMENT IS OFF LINE] RETRUN"FAILURE"
[IF THE NETWORK ELEMENT IS ONE LINE] GENERATE SNMP Get REQUEST
SEND THE SNMP Get REQUEST
SNMP RESPONSE CONTAINING QUERY RESULT
QUERY RESULT

Fig. 3

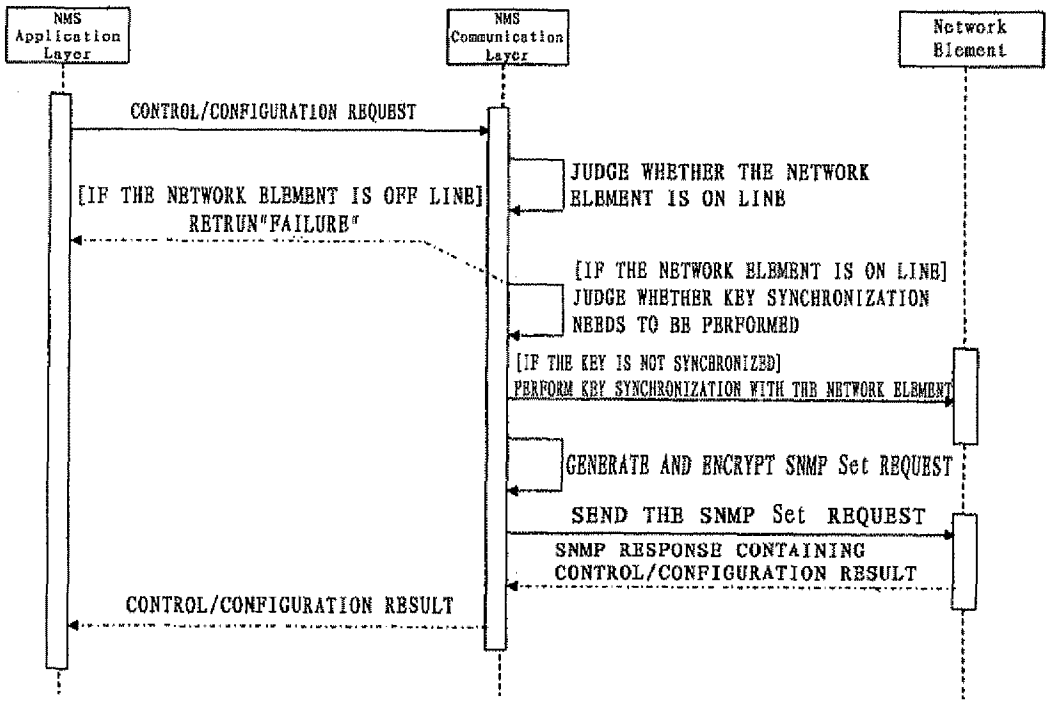

NMS Application Layer
NMS Communication Layer
Network Element
CONTROL/CONFIGURATION REQUEST
JUDGE WHETHER THE NETWORK ELEMENT IS ON LINE
[IF THE NETWORK ELEMENT IS OFF LINE] RETRUN"FAILURE"
[IF THE NETWORK ELEMENT IS ON LINE] JUDGE WHETHER KEY SYNCHRONIZATION NEEDS TO BE PERFORMED
[IF THE KEY IS NOT SYNCHRONIZED] PERFORM KEY SYNCHRONIZATION WITH THE NETWORK ELEMENT
GENERATE AND ENCRYPT SNMP Set REQUEST
SEND THE SNMP Set REQUEST
SNMP RESPONSE CONTAINING CONTROL/CONFIGURATION RESULT
CONTROL/CONFIGURATION RESULT

Fig. 4

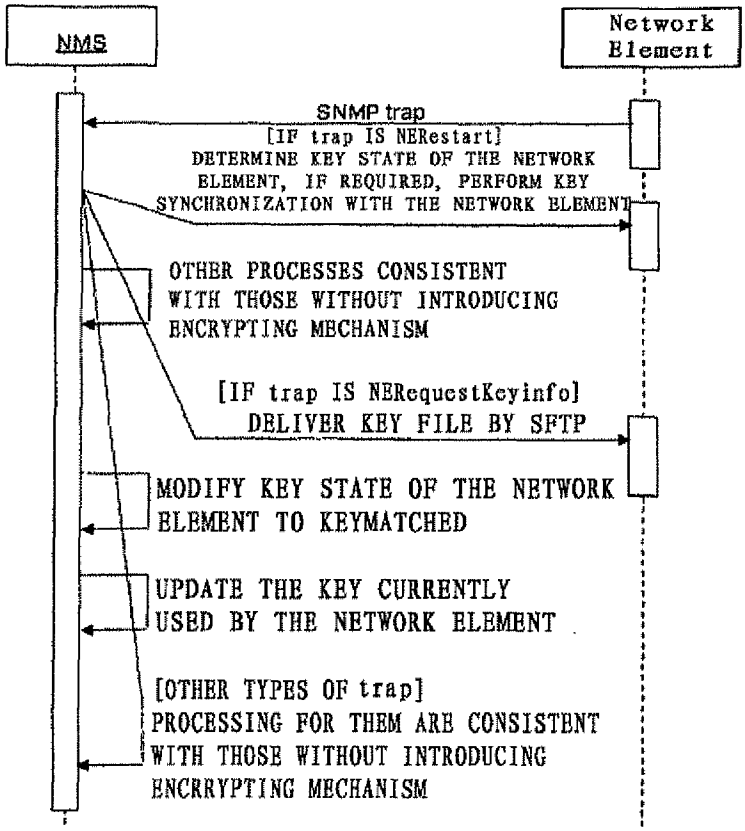

NMS
Network Element
SNMP trap
[IF trap IS NERestart]
DETERMINE KEY STATE OF THE NETWORK ELEMENT, IF REQUIRED, PERFORM KEY SYNCHRONIZATION WITH THE NETWORK ELEMENT
OTHER PROCESSES CONSISTENT WITH THOSE WITHOUT INTRODUCING ENCRYPTING MECHANISM
[IF trap IS NERequestKeyinfo] DELIVER KEY FILE BY SFTP
MODIFY KEY STATE OF THE NETWORK ELEMENT TO KEYMATCHED
UPDATE THE KEY CURRENTLY USED BY THE NETWORK ELEMENT
[OTHER TYPES OF trap] PROCESSING FOR THEM ARE CONSISTENT WITH THOSE WITHOUT INTRODUCING ENCRRYPTING MECHANISM

Fig. 5

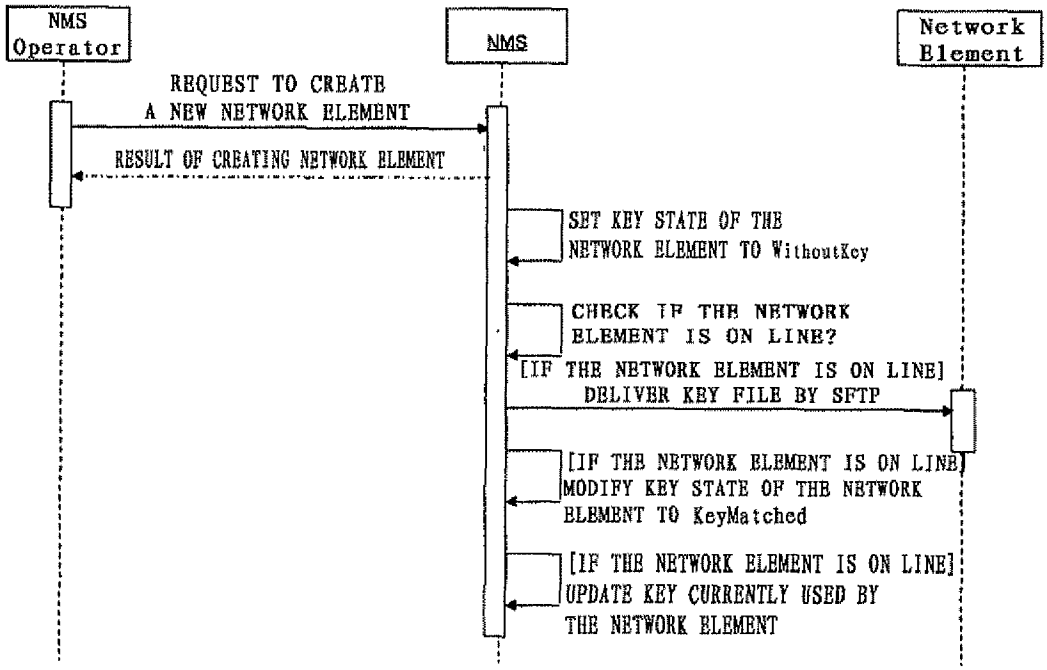

NMS Operator
NMS
Network Element
REQUEST TO CREATE A NEW NETWORK ELEMENT
RESULT OF CREATING NETWORK ELEMENT
SET KEY STATE OF THE NETWORK ELEMENT TO WithoutKey
CHECK IF THE NETWORK ELEMENT IS ON LINE?
[IF THE NETWORK ELEMENT IS ON LINE] DELIVER KEY FILE BY SFTP
[IF THE NETWORK ELEMENT IS ON LINE] MODIFY KEY STATE OF THE NETWORK ELEMENT TO KeyMatched
[IF THE NETWORK ELEMENT IS ON LINE] UPDATE KEY CURRENTLY USED BY THE NETWORK ELEMENT

Fig. 6

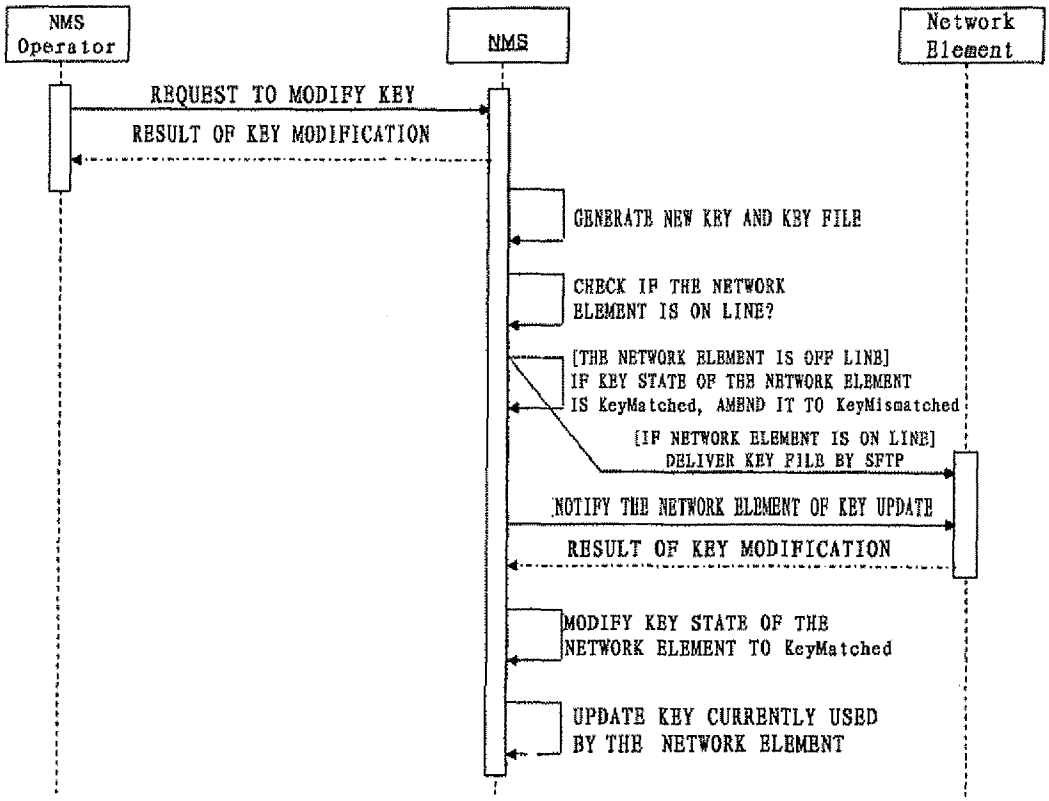

NMS Operator
NMS
Network Element
REQUEST TO MODIFY KEY
RESULT OF KEY MODIFICATION
GENERATE NEW KEY AND KEY FILE
CHECK IF THE NETWORK ELEMENT IS ON LINE?
[THE NETWORK ELEMENT IS OFF LINE] IF KEY STATE OF THE NETWORK ELEMENT IS KeyMatched, AMEND IT TO KeyMismatched
[IF NETWORK ELEMENT IS ON LINE] DELIVER KEY FILE BY SFTP
NOTIFY THE NETWORK ELEMENT OF KEY UPDATE
RESULT OF KEY MODIFICATION
MODIFY KEY STATE OF THE NETWORK ELEMENT TO KeyMatched
UPDATE KEY CURRENTLY USED BY THE NETWORK ELEMENT

Fig. 7