Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2564038 A1 2005/11/17

(21) 2 564 038

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2005/04/29
(87) Date publication PCT/PCT Publication Date: 2005/11/17
(85) Entrée phase nationale/National Entry: 2006/10/23
(86) N° demande PCT/PCT Application No.: US 2005/014990
(87) N° publication PCT/PCT Publication No.: 2005/109715
(30) Priorité/Priority: 2004/04/30 (US60/566,879)

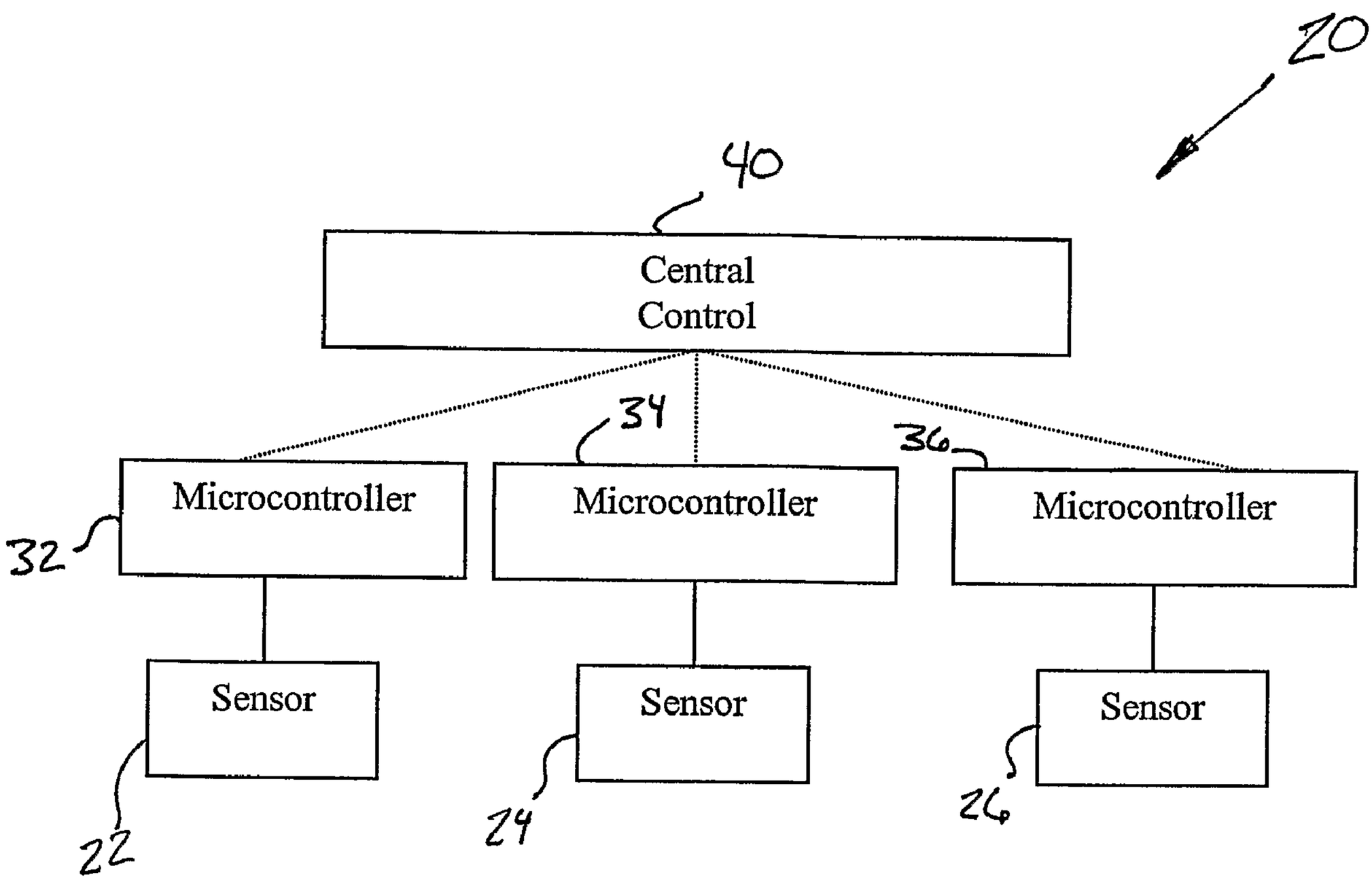
(51) Cl.Int./Int.Cl. *H04K 1/00* (2006.01)

(71) Demandeur/Applicant:
UTC FIRE & SECURITY CORP., US

(72) Inventeurs/Inventors:
RAKOFF, STEVEN BARNETT, CA;
RAM, MANJEET, CA

(74) Agent: OGILVY RENAULT LLP/S.E.N.C.R.L.,S.R.L.

(54) Titre : COMMUNICATIONS DE SYSTEME DE SECURITE FAISANT INTERVENIR UN CRYPTAGE
(54) Title: SECURITY SYSTEM COMMUNICATIONS INCLUDING ENCRYPTION



(57) Abrégé/Abstract:
A security system (20) includes a plurality of sensors (22-26) that provide an indication of a security condition to a corresponding plurality of microcontrollers (32-36). Each microcontroller communicates information regarding the security condition to a central control (40). The communications from the microcontroller include using an elliptical public key encryption for protecting a key associated with the security condition information. In a disclosed example, the security condition information is encrypted using a symmetrical encryption technique.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 November 2005 (17.11.2005)

PCT

(10) International Publication Number
WO 2005/109715 A1

(51) International Patent Classification[7]: H04K 1/00

(21) International Application Number:
PCT/US2005/014990

(22) International Filing Date: 29 April 2005 (29.04.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/566,879 30 April 2004 (30.04.2004) US

(71) Applicant *(for all designated States except US)*: **UTC FIRE & SECURITY CORP.** [US/US]; 9 Farm Springs Road, Farmington, CT 06032 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **RAKOFF, Steven Barnett** [CA/CA]; 279 Hidden Trail, Toronto, Ontario M2R 3S7 (CA). **RAM, Manjeet** [CA/CA]; 4196 Starlight Cres, Mississauga, Ontario L4W 4P9 (CA).

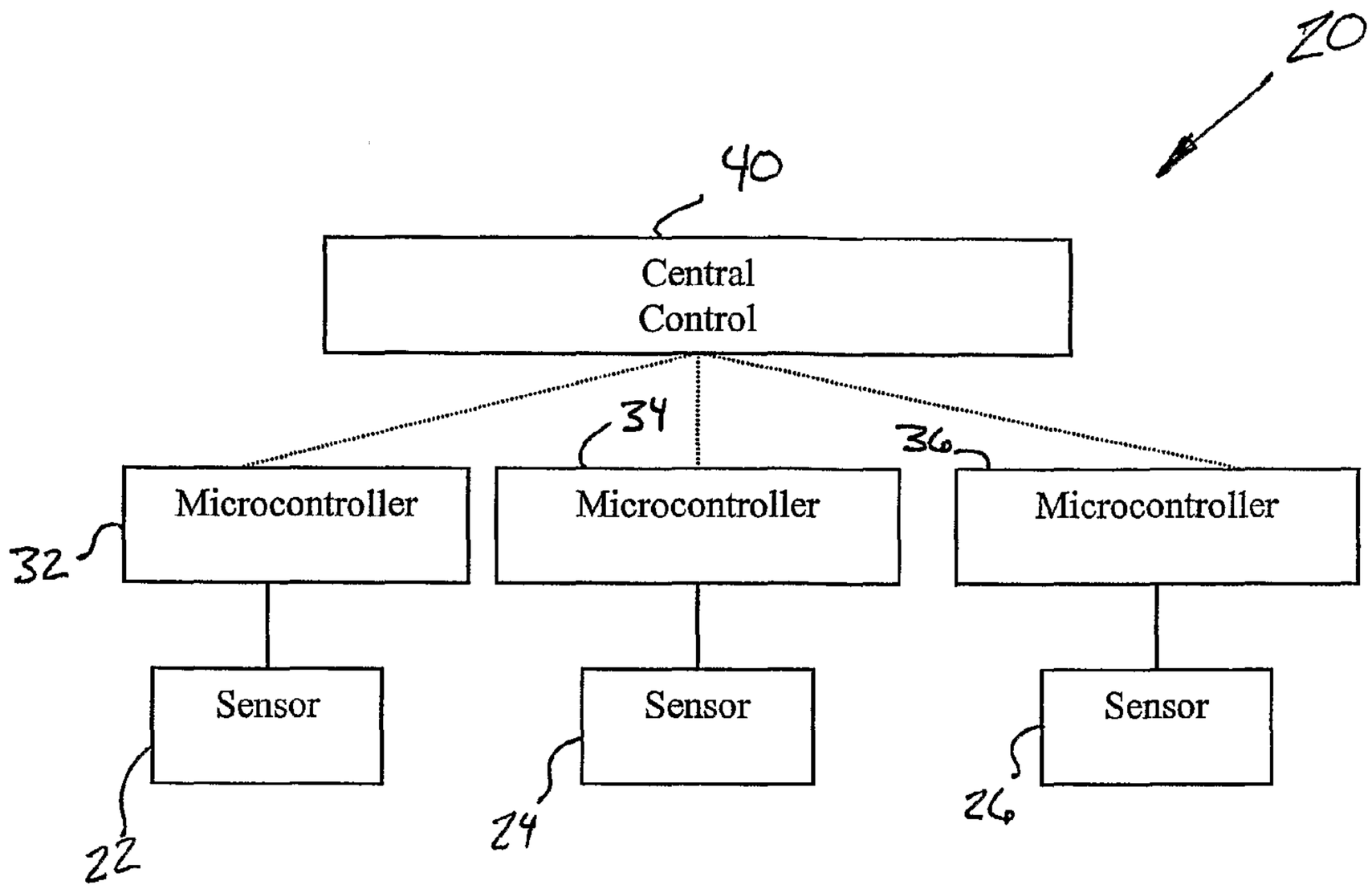
(74) Agent: **GASKEY, David J.**; CARLSON, GASKEY & OLDS, P.C., 400 W. Maple Road, Suite 350, Birmingham, MI 48009 (US).

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



(57) Abstract: A security system (20) includes a plurality of sensors (22-26) that provide an indication of a security condition to a corresponding plurality of microcontrollers (32-36). Each microcontroller communicates information regarding the security condition to a central control (40). The communications from the microcontroller include using an elliptical public key encryption for protecting a key associated with the security condition information. In a disclosed example, the security condition information is encrypted using a symmetrical encryption technique.

WO 2005/109715 A1

WO 2005/109715 A1

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.

SECURITY SYSTEM COMMUNICATIONS INCLUDING ENCRYPTION

Field of the Invention

[0001] This invention generally relates to security systems. More particularly, this invention relates to communicating security system information.

Description of the Related Art

[0002] Security systems are well known and in widespread use. Typical systems include at least one sensor such as a motion detector, camera or a position detector that detects a position of a door or window, for example. The sensors provide information regarding a security condition of an object or location of interest. Typical arrangements include a microcontroller that receives an indication from the sensor regarding the security condition. The microcontroller then communicates information regarding the detected security condition to another location using public communication channels like telephone lines or the internet.

[0003] Such communications from a microcontroller have included some form of protection to prevent unauthorized access to the communications. Known techniques, however, are subject to attack and do not provide a desired level of protection for the communicated information for all circumstances. For example, some microcontrollers do not use any key exchange for purposes of communicating information over a publicly available telephone line or internet connection, for example. Different parse phrase or transmit techniques have been used to provide some level of protection. Other techniques include using a key but providing that key by another route different than the route used for communicating the security condition information. While adding a key in this manner provides additional protection, it has several drawbacks. Providing a key via another route involves additional expense and complexity that reduces the possible efficiency of the security system.

[0004] A significant drawback associated with previous attempts at protecting information communicated by microcontrollers associated with security system devices is that any password or key information typically had to be made available to a variety of individuals who work with the system. This approach makes key

management and key security difficult. The more people who know a password or a key, the less secure it inherently becomes.

[0005] Cryptographic techniques have been developed for protecting information that is communicated in a manner that is susceptible to interception. One known cryptographic technique for protecting a public key associated with transmitted information is known as RSA encryption. Typical arrangements include using public key cryptography techniques include using a slow speed public key encryption to exchange a key for bulk encryption of associated information. For example, RSA encryption is often used to encrypt a key while the known 3DES symmetrical encryption is used for encrypting information associated with the key.

[0006] This approach has not been useful for security systems. The microcontrollers embedded in typical security system devices are not capable of accomplishing RSA encryption unless a special hardware modification were made. The computational and processing requirements associated with public key cryptography such as the RSA encryption technique are too much for a microcontroller to utilize such a technique. Such modifications are not desirable because they introduce additional expense and complexity. A less-secure, bulk or symmetrical encryption technique can be accomplished using a microcontroller, however, that alone does not provide the desired level of security in all circumstances.

[0007] There is a need for an enhanced security system that has better security for communicating security condition information over a publicly available communication channel. This invention addresses that need.

SUMMARY OF THE INVENTION

[0008] This invention includes using an elliptical encryption technique for protecting a key associated with transmitted security condition information that is encrypted using another technique. Using elliptical encryption for protecting the key allows a low cost, low-power microcontroller, such as those typically embedded in security devices, to provide enhanced protection for communicated information.

[0009] One example security system includes at least one sensor that detects a security condition. A microcontroller receives an indication of the security condition from the sensor. The microcontroller communicates information regarding the security condition to another device using a key for protecting the information. The microcontroller uses elliptical encryption for protecting the key.

[00010] One example security system includes a plurality of microcontrollers that each use an elliptical public key encryption for protecting the key and ultimately protecting the communicated information regarding the security condition. Utilizing the disclosed approach provides significant advantages from an entire system standpoint when one considers that multiple microcontrollers can now be efficiently used with greater security compared to previous arrangements.

[00011] An example method of communicating information in a security system includes associating a key with information regarding a security condition. The key is encrypted using an elliptical encryption technique. The information regarding the security condition is encrypted using another technique. In one example, the information regarding the security condition is encrypted using a symmetrical encryption technique.

[00012] The various features and advantages of this invention will become apparent to those skilled in the art from the following detailed description. The drawing that accompanies the detailed description can be briefly described as follows.

BRIEF DESCRIPTION OF THE DRAWING

[00013] Figure 1 schematically illustrates selected portions of a security system designed according to an embodiment of this invention.

DETAILED DESCRIPTION

[00014] This invention includes using elliptical encryption techniques for protecting a key associated with communicated information regarding a security condition. The information itself may be encrypted using another encryption technique such as a symmetrical encryption technique. Using an elliptical encryption technique for protecting the key allows a typical low cost, low-power microcontroller embedded in a security system device to provide enhanced communication protection without requiring modification to the microcontroller or the introduction of a higher power, more expensive controller to accommodate the complexities associated with other types of encryption.

[00015] Figure 1 schematically shows selected portions of a security system 20. A plurality of sensors 22, 24 and 26 provide information regarding various security conditions at various locations. Example sensors include cameras, motion detectors or position detectors that operate in a known manner. In one example, the plurality of

sensors are located at different positions within a building or complex. In another example, the sensors 22-26 are located at buildings that are remote from each other.

[00016] Each sensor provides an indication regarding a detected security condition (such as an open door or motion within a particular area, for example) to a microcontroller. In this example, the sensor 22 communicates with a microcontroller 32, the sensor 24 communicates with a microcontroller 34 and the sensor 26 communicates with a microcontroller 36.

[00017] Each of the microcontrollers communicates information regarding the sensed or detected security condition to a central control device 40. In one example, the central control device is at a remote location compared to that where the sensors and microcontrollers are positioned. Communications between the microcontrollers 32-36 and the central control device 40 are accomplished in one example using publicly available communication facilities such as telephone lines or the internet. To protect these communications, each microcontroller 32-36 associates a key with the information regarding the security condition to be communicated to the central control 40.

[00018] In one example, each microcontroller 32-36 encrypts the key associated with the security condition information using an elliptical public key encryption technique. The microcontrollers 32-36 and the central control 40 utilize the elliptical encryption for initially exchanging the key that allows both devices to have a symmetrical key for certification of the associated, communicated security condition information. Prior to the first elliptically encrypted key exchange, the microcontrollers use elliptical encryption for certification where the microcontrollers 32-36 validate the central control 40.

[00019] In one example, each microcontroller 32-36 also encrypts the security condition information but uses another type of encryption. In one example, a known bulk or symmetrical encryption technique is used for encrypting the security condition information to protect that information. The central control 40 uses an appropriate technique for deciphering that information after certifying that a proper key exchange has taken place.

[00020] With the disclosed example, a low-cost, low-power microcontroller is capable of providing the communication in an encrypted manner that fits within the typical capability of such microcontrollers and still provides better security then relying purely upon symmetrical encryption for the entire communication. The

disclosed example provides the ability to have secure communications over publicly available telephone lines or the internet, for example, while still working within the constraints typically imposed by the capability of low cost, low-power microcontrollers.

[00021] A significant advantage to the disclosed example is that it allows for existing security system devices such as control panels, access key pads and other system interface devices that have embedded low-power microcontrollers to be suitably programmed to accomplish the results provided by the disclosed example embodiment. This does not introduce any additional cost into the hardware of the system. Moreover, the complexities otherwise associated with trying to manage key information in security systems that rely upon a plurality of microcontrollers are essentially eliminated when employing the disclosed example embodiment. There no longer is any need for an individual or a plurality of individuals to periodically update key information for a plurality of microcontrollers in an attempt to maintain ongoing security. By utilizing elliptical encryption techniques for key information, that key information is far more secure and can be kept constant for a much longer period of time.

[00022] The preceding description is exemplary rather than limiting in nature. Variations and modifications to the disclosed example may become apparent to those skilled in the art that do not necessarily depart from the essence of this invention. The scope of legal protection given to this invention can only be determined by studying the following claims.

CLAIMS

We claim:

1. A security system, comprising:

at least one sensor that detects a security condition; and

a microcontroller that receives an indication of the security condition from the sensor and communicates information regarding the security condition to another device using a key for protecting the information, the microcontroller uses elliptical encryption for protecting the key.

2. The security system of claim 1, comprising a plurality of said microcontrollers, each using elliptical encryption for an associated key.

3. The security system of claim 2, comprising a central control device that communicates with the plurality of microcontrollers and uses the elliptically encrypted key for certifying the communicated information.

4. The security system of claim 1, wherein the microcontroller uses symmetrical encryption for encrypting the communicated information.

5. The security system of claim 4, wherein the communicated information comprises an alarm protocol.

6. A method of communicating information in a security system having at least one microcontroller that communicates information regarding at least one security condition, comprising the steps of:

associating a key with information regarding the security condition;

encrypting the key using elliptical encryption; and

encrypting the information regarding the security condition.

7. The method of claim 6, including encrypting the information regarding the security condition using another encryption that is different than the elliptical encryption.

8. The method of claim 7, including using a symmetrical encryption for encrypting the information regarding the security condition.

9. The method of claim 6, including communicating the encrypted key and the encrypted information regarding the security condition to a central control device and deciphering the key to certify the communicated information regarding the security condition.

10. The method of claim 6, comprising providing a plurality of sensors each for detecting at least one security condition, providing a plurality of microcontrollers for receiving an indication from corresponding sensors, and using the elliptical public key encryption at each of the microcontrollers.

11. The method of claim 6, including transmitting the encrypted key and the encrypted information in a single transmission.

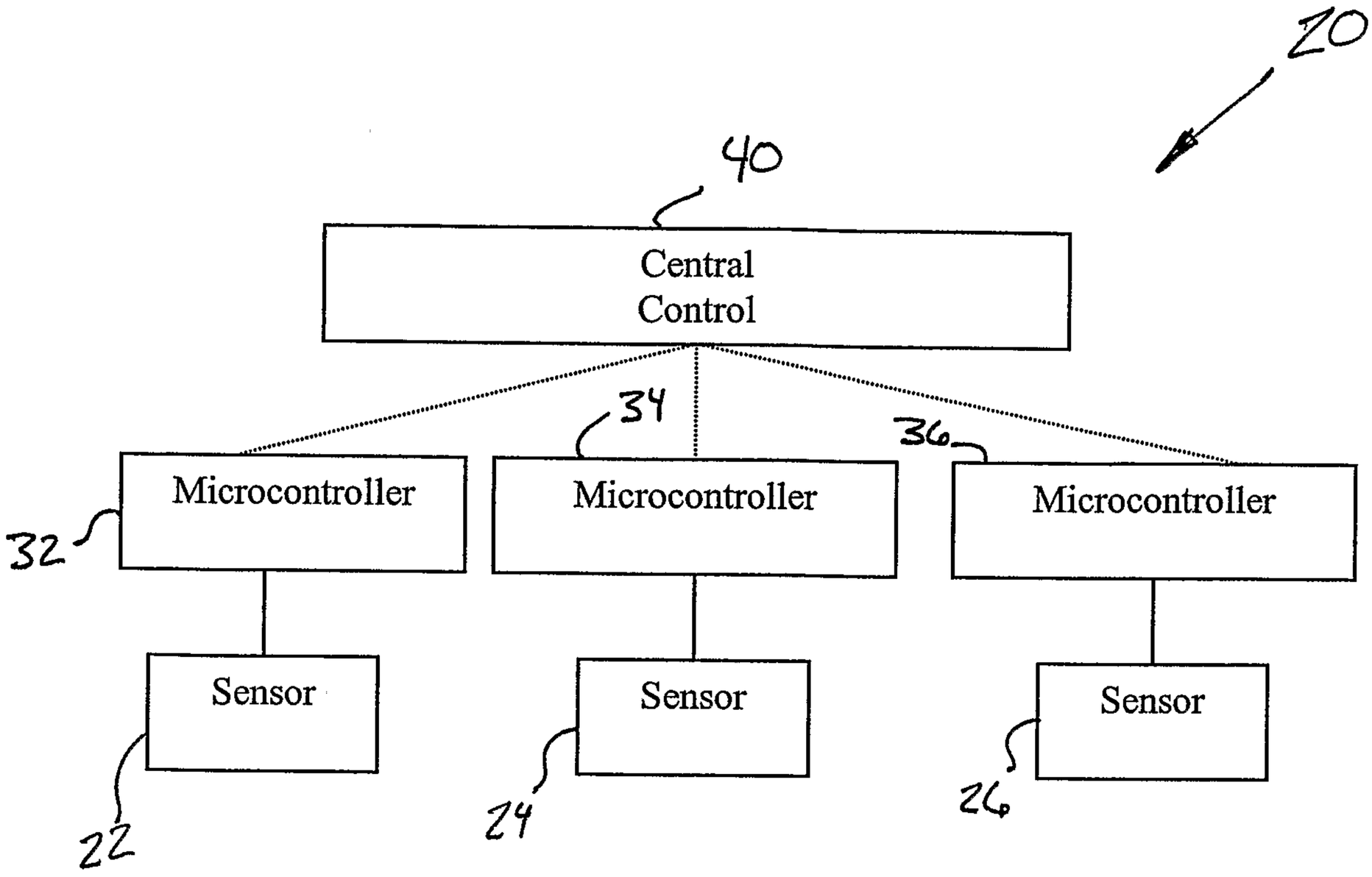
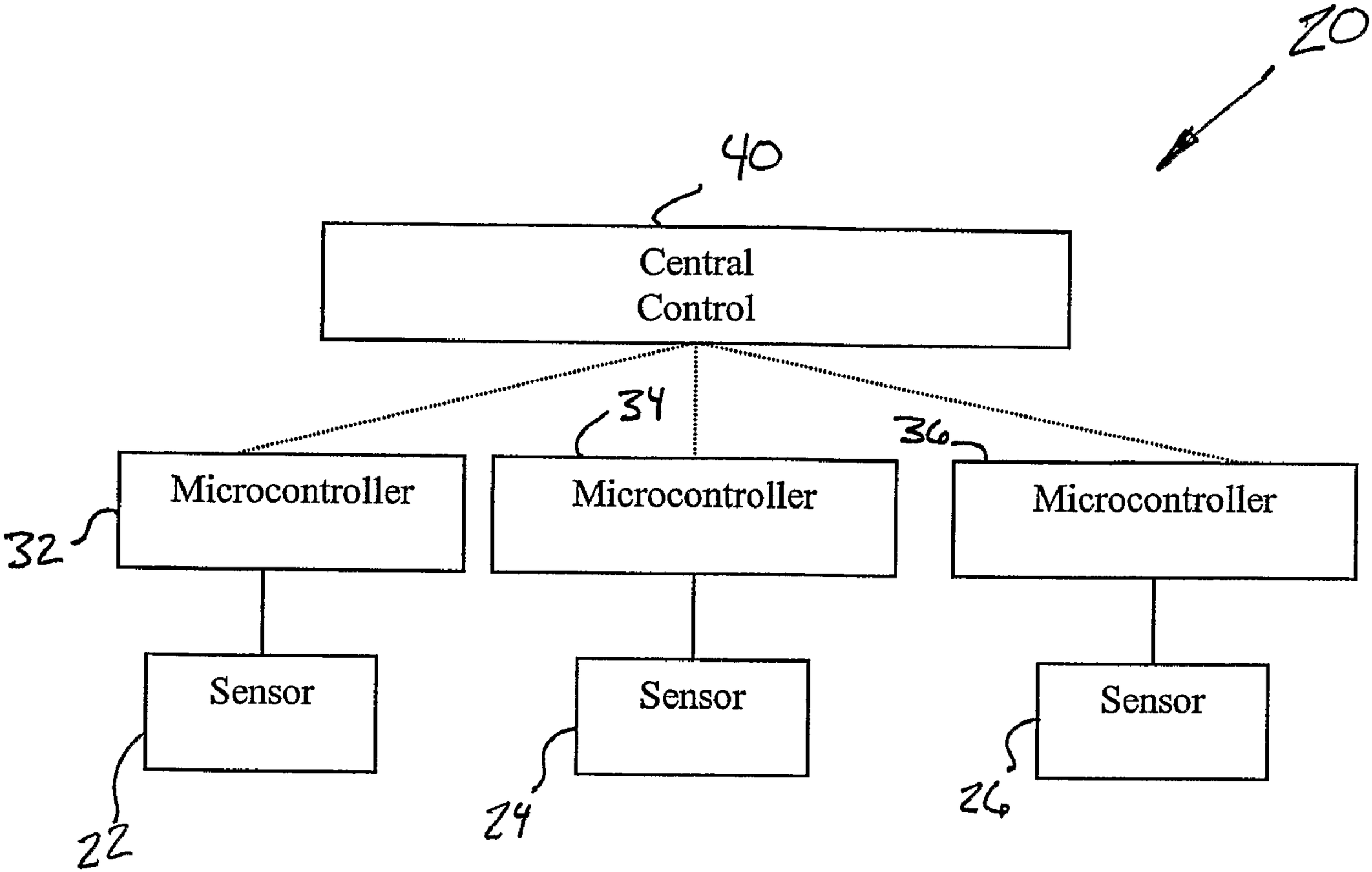

20
40
Central
Control
34
36
Microcontroller
Microcontroller
Microcontroller
32
Sensor
Sensor
Sensor
22
24
26

Fig 1


20
40
Central
Control
34
36
Microcontroller
Microcontroller
Microcontroller
32
Sensor
Sensor
Sensor
22
24
26