A Novel Method for a Reliable and Secure Building Monitoring, Warning and Remote Controlling System

Mohammed M. Jasim, Oleg Vector
Middle East University
Amman, Jordan
{Mohammed, joseph.morris}@computing.dcu.ie

ABSTRACT: *Modern communication and data transaction technologies offered good solutions to important problems appeared in human modern life. Several researches tried to find solutions to the building remote control, monitoring and alarming system using the modern technology. Many of them proposed methods to solve these problems. However, these solutions created new problems regarding security and reliability efficiency. In this work, a method to solve the security and reliability for a building remote control, monitoring and alarm system will be proposed.*

Keywords: Monitoring, Alarming, Remote Controlling, Internet, GSM, Encryption, Decryption

Received: 10 May 2013, Revised 8 June 2013, Accepted 14 June 2013

1. Introduction

Secrecy of information is being considered as a high priority issue since the ancient world. The information that contains messages has two cases of secrecy weaknesses; storage or saving of the message, and message transfer. From the ancient world, human faced a big deal to hide the transferred message from source to destination. Initially, focal messages were very power full, but it has many limitations and costs much more. In fact, not all focal messages are possible to be transmitted. This depends on many factors, including find the message holder people which is considered to be very danger issues and needs special treatment. Also, the transfer of human is costing much more that transferring of written message which is possible to be attached with many different methodologies.

The security of the message was raised from the importance and secrecy of the data that included in that message. So, the earlier human methodologies was very simple and based on hiding the message either by the use of vocal messages or by putting the paper that the messages was written on into a very secure location.

In modern centuries, a common practice that had been used for very long time with some of efficiency is to hide the information using chemical reactors of ink materials [1], it was known as invisible inks. Sources for invisible inks include milk, vinegar, fruit juices and such. Such technique was invented by a German intelligence [2]. That was to hide of the message itself, which is commonly known as Steganography. The more popular techniques that used to add security levels on the secure messages is to hide the message contents while the message itself is not hidden.

Another issue that faces all people those are used to send critical messages over transport layer is the failure of communication medium. When using internet, the internet service provider (ISP) in many cases do not offer a reliable internet service even in

browsing. This makes the dependency on internet to be very risky. In Jordan, the possibility of keeping the internet connected for a couple of continuous hours is seems to be impossible. Instead, it disconnects and connects much time a day. So, if the user depend on the internet ISP only to transfer critical messages that will be a big mistake.

This paper presents a solution to the building monitoring, alarming and remote controlling system. This building could be a hospital, a hotel, a prison, a bank, etc., which present a very critical problem due to monitoring, alarming and remote controlling of their appliances. That in order to control them a reliable and secure system is highly needed.

To make hybrid decision-making using hybrid network transport applications. The basic is internet and the backup is mobile GSM communications. In the case of failure of internet, the cellular mobile communication is capable of sending SMS instead.

Critical message could fall in two categories [3]; the first is secret contents messages which is used by security directorates and department in the most cases, also, it is being used by the companies and institutes to keep the secret data confidential The second type is the priority messages which is not really required to be secret, but it is must to reach the destination from the source.

The first type of messages is hardly required to be secret and confidential. The confidentiality of those messages is much important than the reliability of the transfer itself. This means that, even though the transfer may face much failure, it should be at top secrecy level to keep secret and no one can reach its contents.

The control messages is the type of messages that includes automatic commanding of physical system or computer system, including the messages that contains a type of data that affects the decision making process of the computerized system. This type of messages are a combination of the two critical messages categories; it is required to be secret to prevent any intrusion from hacking or affecting the decision making process in any circumstances. In addition, it is top priority to make reliable transfer that could be in real time in many cases [4].

In this paper, it is aimed to propose high level of secure adaptive algorithm to enable transfer a secret data over internet and short messages service (sms) of GSM mobile communication. The data is intended to have high security by contributing mathematical based Cryptographic encryption of the sent message and decryption of the received one. Thus, the message context will be hidden.

In order to achieve high level real security, this paper considers multi-level of security based on the multi-level data encryption. The message context will be encoded and encrypted. Moreover, the command that is included inside the message will have a unique form.

Two transfer mediums are being used in hybrid form, the internet and SMS of the GSM mobile communications, where in the case of internet failure either due to local internet service provider or due to network traffics, the message could be sent via SMS directly. Thus, in the success factor will be doubled and the missing rates of the command messages will be significantly minimized.

The message also will contain a unique header to identify the sender and the purpose of the message. The decision will be made upon special format of the message contents. Hence, the target application system is domestic home operation and control, so, the control strategies and interfacing with the home measurements and actuators will be described in this paper too.

Beside this section, related cryptography methods and algorithms will be explained in the second section, in the third section, the proposed algorithm will be explained, then the experimental results will be discussed in the fourth section, finally a summary and conclusion of the work will be mentioned in the fifth section.

2. Data Transaction Algorithm

The rise ارتفاع up of the modern technology increases الزيادات the problem of data security and enlarges the problem of hiding the message data in old methodologies. In fact (الحقيقه), the paper messages become rare (نادر) in the age of cellular communications and internet technology. This state's trigger (تحريك) the modern computer researchers to keep going on researches in encryption / decryption and data security to hide the message contents in effective way in order to achieve a rigid ((صلب-قاس) secure

message transfer in contrast (تباين) with hacking property in addition to the problems of communication media (internet and cellular phone communications).

The secret messaging in ancient world and modern technologies are categorized to two fields; cryptography and Steganography. The Greek origin of the Steganography is combined of two words [5] (Steganos) and (Graphei). "*Steganos*" means covered or hidden, where the word "*Graphei*" means writing, so, the Steganography means "*Hidden Writing*". From the same concept, the Cryptography are derived from the Greek origin of two words [6]; (Cryptology) which means secret, and (Graphei), this is collecting the meaning of "*Secret Writing*". Secret writing is the implementation of writing in unknown syntax.

Boukerche et.al, in their work [7], studies the possibility of hiding information in ad-hoc network, by establishing a trust among mobile nodes and avoid untrusted nodes during the route discovery process. By this way, they aimed to allow only trustworthy nodes to participate in data transaction.

On the other hand, Huang et al [8], proposed an encrypted data algorithm scheme for wireless sensor networks (WSN), their method provided security and privacy. Moreover, the duplicate instances of original readings will be aggregated into single packet. They found solutions for plain-text attacks, ciphertext-only attacks and man-in-the middle attacks. Moreover, they showed that their method reduces communication overhead.

In their work [9], Tews et al, described two attacks on IEEE 802.11based wireless LANs. The first one is an improved key recovery attack on WEP, which reduces the average number of packets an attacker has to intercept to recover the secret key. Moreover, they presented the second one as the first practical attack on WPA secured wireless networks, besides launching a dictionary attack when a weak pre-shared key (PSK) is used. They analyzed the attacks, in order to understand them to be able to develop a secure solution to prevent them.

Tewari et al, in their work [10], proposed a new protocol using multifactor authentication system that is both secure and highly usable. Their method was based on transaction identification code and SMS to enforce extra security level with the traditional authentication system. Which provided a highly secure environment that is simple and applicable. Their method provided two-way of authentication.

3. Proposed Model

The importance of controlling the appliances in important facilities like banks, hospitals and such facilities, forced the researchers to keep searching for solutions to keep controlling them, any time and from anywhere. If the temperature inside a hospital was increased or decreased, there is a critical problem will happen. The same thing, if a door for a bank department was opened after the working time, this means that a critical thing was happened there and needs an immediate reaction . Thus, a reliable and secure monitoring, alarming and remote controlling system is urgently (حاجه ملحه) needed to be applied.

As shown in figure 1, above, the proposed methodology to solve this problem is divided into two categories: The first one is to solve the problem of security and the second one, is to solve the problem of reliability.

3.1 Reliability Problem

In order to achieve the reliability for the mentioned ذكر system, an active/passive method is proposed. Initially there should be a server mounted inside the building and connected to the appliances, this server contains a controller, which controls the appliances, such as increasing or decreasing the air conditions' temperature, or turning on or off an appliance.

On the other hand, there should be sensors connected on the appliances to send the logs سجلات to the server, which analyze the logs and send an alarm to the controller to take the suitable مناسب action. However, this server is connected to the outside world through two channels. The first one is by using an Ethernet card to connect it to the internet, which assumes يفترض that this server has a public IP address in order to be accessed from the internet. The second one is by using a GSM modem, which contains a SIM card to allow the server to communicate and be communicated through the GSM network.

The controller is configured with a routing protocol, which initially define the two routes; the internet and the GSM. Moreover, gives a priority to each one, in a preemptive وقائيه way. Such as, when the channel with high priority turns down, or becomes unavailable, the controller turns the traffic to the other channel, until the first one returns up, then the server returns the traffic

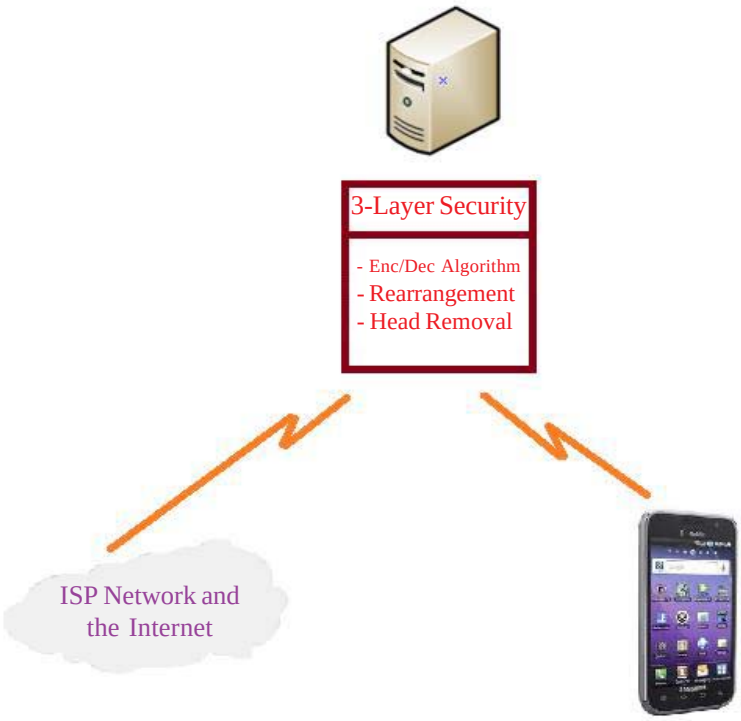

Figure 1. Reliable and Secure Solution Components

to it. By this way, the server ensures that the traffic always has a path to the outside world to send the alarm and log messages and receives the controlling instructions.

However, this reliable solution brings another problem, that using the internet and the GSM network is susceptible to hackers, sniffers and spywares, which turns the attention to look for a secure way for data transaction.

3.2 Security Problem

Security is a major issue for the system under study, as if hackers caught القبض the instruction and the destination for controlling the appliances of the building, it would be easy for them to send false instructions or even stop the monitoring system, which cause a real and dangerous problem. Thus, it is very important when developing a complete solution to the monitoring, alarming and remote controlling system, to turn the focus on the security issues.

The proposed security algorithm is based on encryption/decryption method. In which the data are hidden before they are transmitted. The algorithm contains three layers of security to make it more difficult for any attacker to be able قادر to break it.

The first layer of security is to encrypt the instruction using a new mathematical equation after mapping each character to binary. This new equation is very complex which turns the binary characters to meaningless numbers; this equation is variable, which means that for every character the operands of the equation will be changed. Moreover, it uses random variables which seeds are generated in different way from character to another.

The reverse and the seeds for this equation are stored as a certificate file, which stored only inside the server and the authenticated موثق, agents, and not sent with the packet. In this way, no one will be able to reverse the equation معادله and restore the encrypted instructions.

The second layer of security is after encrypting the data; each character will have different position in the series, based on a positioning algorithm, which is known only to the server and the authentic agents. Therefore, the encrypted characters will have different positions before being sent to the destination.

The third layer of security is to remove the head of the packet, which contains the sender and receiver information, in addition to the type of the packet, this layer, prevents any unauthenticated side from understanding this packet or even knowing its destination.

By this algorithm, if the attacker was able to break the first layer he/she will not be able to break the second or the third one, which give more strength to the proposed algorithm and ensure the security in addition to the reliability of this system.

4. Conclusions and Summary

In this work, the monitoring, alarming and remote controlling system was proposed for important facilities such as hospitals, banks, prisons, etc., which contain important appliances that need to be fully controlled any time and from anywhere; in addition, they should be always monitored.

To solve this problem, researchers developed several solutions but their solutions lacked the reliability and security. In this work, a complete solution that solved the reliability and security issues for the problem under study was proposed.

The proposed method was divided into two subsystems: in the first one the reliability problem was solved by connecting this system to two channels, the internet and the GSM networks, for data transaction. By this way a reliable and available system is ensured.

The second subsystem, solved the security problem. The proposed security algorithm contains three layers of security: the first one, is an encryption/decryption algorithm, which encrypt the data before transmitting them.The second one, is the rearrangement اعادة ترتيب of the characters. The third one is the removal of the header of the packet before transmitting it. By this three-layer security algorithm a secure, in addition to a reliable building monitoring, alarming and remote controlling system is ensured.

References

[1] Kazmaier, Peter, M., et al. (2013). Solid phase change fluorescent ink and ink sets. (2678341). 18 Jun.

[2] Auslander, Judith, D., William Berson. (1996). Bar codes using luminescent invisible inks. U.S. Patent, (5, 542, 971). 6 Aug.

[3] Kaufman, Charlie, et al. (2010). Internet key exchange protocol version 2 (IKEv2). RFC 5996, September.

[4] Wu, Zhaohui, Mark Pagell. Balancing priorities: Decision-making in sustainable supply chain management. *Journal of Operations Management*, 29.6, 577-590.

[5] Johnson, Neil, F., Sushil Jajodia. Exploring steganography: Seeing the unseen. *IEEE computer*, 31.2 (1998): 26-34.

[6] Singh, Simon. (2011). The code book: the science of secrecy from ancient Egypt to quantum cryptography. Random House Digital, *Inc*.

[7] Boukerche, Azzedine, et al. (2004). A novel solution for achieving anonymity in wireless ad hoc networks. *In*: Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks. *ACM*.

[8] Huang, Shih-I., Shiuhpyng Shieh, Tygar, J. D. (2010). Secure encrypted-data aggregation for wireless sensor networks. *Wireless Networks*, 16.4, 915-927.

[9] Tews, Erik, Martin Beck. (2009). Practical attacks against WEP and WPA. *In*: Proceedings of the second ACM conference on Wireless network security. *ACM*.

[10] Tiwari, Ayu, et al. (2011). A Multi-Factor Security Protocol for wireless payment-secure web authentication using mobile devices. arXiv preprint arXiv:1111.