**SECURITY SENSOR APPLICATION: BENEFITS AND CHALLENGES IN OUR SOCIETY**

**MUHAMMAD MUBARAK MUSA**

**(ST/CS/ND/20/128)**

**A SEMINAR PAPER PRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE AND TECHNOLOGY, FEDERAL POLYTECHNIC MUBI, ADAMAWA STATE, NIGERIA**

**NOVEMBER, 2022**

**SECURITY SENSOR APPLICATION: BENEFITS AND CHALLENGES IN OUR SOCIETY**

**MUHAMMAD MUBARAK MUSA**

**(ST/CS/ND/20/128)**

**A SEMINAR PAPER PRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE AND TECHNOLOGY, FEDERAL POLYTECHNIC MUBI, ADAMAWA STATE, NIGERIA**

**IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF NATIONAL DIPLOMA (ND) IN COMPUTER SCIENCE**

**NOVEMBER, 2022**

**Abstract**

*Security Sensor Application has important applications such as remote environmental monitoring and target tracking. The design of a SSA depends significantly on the application and the environment, the application’s design objectives, cost, hardware and system constraints, routing mechanism. Security Sensor Application (SSA) have gained worldwide attention in recent years, particularly with the proliferation in Micro-Electro-Mechanical Systems technology which has facilitated the development of smart sensors and miniaturized sensor. The sensor miniaturization, with limited processing and computing resources are inexpensive compared to traditional sensors. Now a days, Sensor miniaturization is only possible because of the current state of the art in nanotechnology.*

**Keywords:** Security, Sensor, Challenges, Nanotechnology, Routing.

**Introduction**

Security Sensor application is the condition of being protected against danger or loss. In the general sense, security sensor is a concept similar to [safety](http://en.wikipedia.org/wiki/Safety). The nuance between the two is an added emphasis on being protected from dangers that originate from outside. Individuals or actions that encroach upon the condition of protection are responsible for the breach of security. The word "security" in general usage is synonymous with "safety," but as a technical term "security" means that something not only *is secure* but that it *has been secured.* One of the best options for providing good security is by using a technology named security sensor applications (Meena & Somkuwar, 2014).

A security sensor application can be defined as a computing device that does a specific focused job. Appliances such as the air-conditioner, VCD player, DVD player, printer, fax machine, mobile phone etc. are examples of security sensor applications. Each of these appliances will have a processor and special hardware to meet the specific requirement of the application along with the embedded software that is executed by the processor for meeting that specific requirement (Wang et al., 2008).

Gharaei et al. (2017), Security sensor applications do a very specific task, they cannot be programmed to do different things. Security sensor applications have very limited resources, particularly the memory. Generally, they do not have secondary storage devices such as the CDROM or the floppy disk. Security sensor applications have to work against some deadlines. A specific job has to be completed within a specific time. In some security sensor applications, called real-time systems, the deadlines are stringent. Missing a deadline may cause a catastrophe-loss of life or damage to property. Security sensor applications are constrained for power. As many security sensor applications operate through a battery, the power consumption has to be very low.

Some security sensor applications have to operate in extreme environmental conditions such as very high temperatures and humidity (Zeng & Yan, 2014).

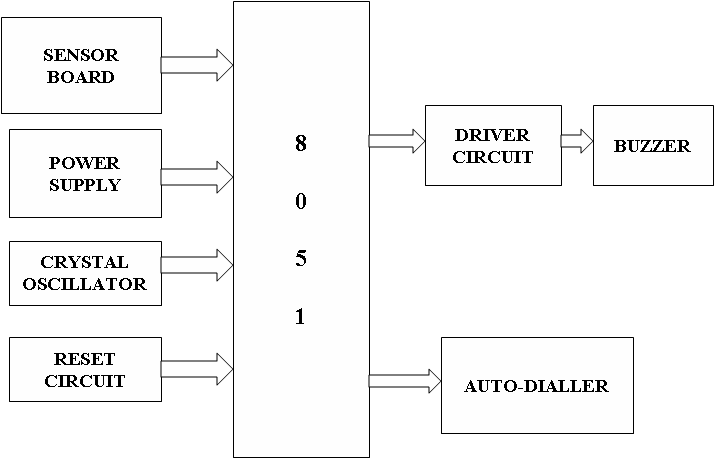
**Literature Review**

Wang et al. (2008), wireless sensor network nodes are generally located in security-sensitive areas and unsupervised environments, which makes data fusion of wireless sensor network easy to face various security threats. Under the influence of low energy cost, a complete security mechanism must be provided to ensure data security. Data integrity scheme and data rolling scheme are common data integration schemes in current wireless sensor networks. The former is based on data integrity, while the latter is based on data privacy. And in order to guarantee the data security, cooperate more symmetric cipher algorithm of data fusion method by encryption scheme, this scheme has high applicability to advantage, but also exists the shortage of the aggregation point too expensive, in order to reduce the energy consumption of the present scheme, can be targeted to adjust intermediate node in the process of data transmission, make its not decrypt the received data, and through the aggregation number, will receive the data packet and forward their own data encryption to the parent node, by omitting decrypted and encrypted link again, can greatly reduce energy consumption, and this change will not affect the network security, This new protection scheme with both security and low energy consumption is the data security fusion technology (Hoang, 2014).

In order to ensure that the data fusion technology can better serve the security of wireless sensor networks, a data fusion security scheme based on trust mechanism should be specifically designed, in which the direct trust factor and mutual trust factor are composed of trust management factors of wireless sensor networks. Through to observe the motion of the monitoring node module, pretreatment and calculate the network monitoring results, can be based on the direct trust mentioned in the calculated value and build the trust value of the complete each node comprehensive letter stated value calculation, calculation result will be sent to the trust decision module described in the fusion processing, can carry out pertinent fusion processing. In the fusion process, in order to make the member nodes trust, the sampled fusion nodes should be watched by the cluster member nodes according to their behaviors (Prema & Narmatha, 2016).

In combination with data fusion byte points, the result set nodes should be calculated and evaluated, and the base station should be responsible for the final decision. In comprehensive trust value computation link, according to the integration of each node to store trust direct, indirect trust value, direct trust value, can according to the trust value and the current trust history value synthesis method of weighted summation, the complete direct trust value computation, indirect trust value this process must be applied to include weighted factor is recommended (Hoang, 2014).

In order to avoid the calculation error of indirect trust, it is necessary to pay more attention to whether the weighted factor is involved in the calculation, and the influence of the trust mechanism characteristics of periodic behaviors and the recommendation level of historical trust on the trust of fixed nodes should also be paid attention to. The specific formulation of data fusion security scheme should be combined with the need to protect privacy. In order to ensure the privacy of wireless sensor network, encryption processing method is generally adopted, and data fusion protection algorithm can also be adopted. This paper proposes to adopt an improved SMART scheme based on the traditional SMART scheme. Traditional SMART solutions by data detection, segmentation and convergence order of three phase, considering the cost of the scheme in recent years, and reduce the cost cannot adopt the way of lower safety threshold, so need to choose plan of improvement of SMART, with specific network initialization, data transmission, data fusion, to be able to better service in wireless sensor network security, network initialization should first establish the relief valve, and establish the data fusion tree. Data transmission needs to allocate different transmission time for each node group to avoid location and information exposure. Therefore, when passing through intermediate node I, the packet will not be forwarded directly, but will be forwarded after passing through random cache time. Data fusion is based on data fusion tree expansion, and the key is used to add and decrypt data (Vijayarajeswari *et al.* 2016).



**Figure 1:**

**Application Security Sensor Application**

Parenreng and Kitagawa (2017), nearly 99 per cent of the processors manufactured end up in security sensor applications. The security sensor application market is one of the highest growth areas as these systems are used in very market segment- consumer electronics, office automation, industrial automation, biomedical engineering, wireless communication, data communication, telecommunications, transportation, military and so on.

1. **Consumer appliances**: At home we use a number of security sensor applications which include digital camera, digital diary, DVD player, electronic toys, microwave oven, remote controls for TV and air-conditioner, VCO player, video game consoles, video recorders etc. Today’s high-tech car has about 20 security sensor applications for transmission control, engine spark control, air-conditioning, navigation etc. Even wristwatches are now becoming security sensor applications. The palmtops are powerful security sensor applications using which we can carry out many general-purpose tasks such as playing games and word processing.
2. **Office automation:** The office automation products using security sensor applications are copying machine, fax machine, key telephone, modem, printer, scanner etc.
3. **Industrial automation**: Today a lot of industries use security sensor applications for process control. These include pharmaceutical, cement, sugar, oil exploration, nuclear energy, electricity generation and transmission. The security sensor applications for industrial use are designed to carry out specific tasks such as monitoring the temperature, pressure, humidity, voltage, current etc., and then take appropriate action based on the monitored levels to control other devices or to send information to a centralized monitoring station. In hazardous industrial environment, where human presence has to be avoided, robots are used, which are programmed to do specific jobs. The robots are now becoming very powerful and carry out many interesting and complicated tasks such as hardware assembly.
4. **Medical electronics**: Almost every medical equipment in the hospital is an security sensor application. These equipment include diagnostic aids such as ECG, EEG, blood pressure measuring devices, X-ray scanners; equipment used in blood analysis, radiation, colonscopy, endoscopy etc. Developments in medical electronics have paved way for more accurate diagnosis of diseases.
5. **Computer networking**: Computer networking products such as bridges, routers, Integrated Services Digital Networks (ISDN), Asynchronous Transfer Mode (ATM), X.25 and frame relay switches are security sensor applications which implement the necessary data communication protocols. For example, a router interconnects two networks. The two networks may be running different protocol stacks. The router’s function is to obtain the data packets from incoming pores, analyze the packets and send them towards the destination after doing necessary protocol conversion. Most networking equipments, other than the end systems (desktop computers) we use to access the networks, are security sensor applications
6. **Telecommunications**: In the field of telecommunications, the security sensor applications can be categorized as subscriber terminals and network equipment. The subscriber terminals such as key telephones, ISDN phones, terminal adapters, web cameras are security sensor applications. The network equipment includes multiplexers, multiple access systems, Packet Assemblers Dissemblers (PADs), sate11ite modems etc. IP phone, IP gateway, IP gatekeeper etc. are the latest security sensor applications that provide very low-cost voice communication over the Internet.
7. **Wireless technologies**: Advances in mobile communications are paving way for many interesting applications using security sensor applications. The mobile phone is one of the marvels of the last decade of the 20’h century. It is a very powerful security sensor application that provides voice communication while we are on the move. The Personal Digital Assistants and the palmtops can now be used to access multimedia services over the Internet. Mobile communication infrastructure such as base station controllers, mobile switching centers are also powerful security sensor applications.
8. **Insemination:** Testing and measurement are the fundamental requirements in all scientific and engineering activities. The measuring equipment we use in laboratories to measure parameters such as weight, temperature, pressure, humidity, voltage, current etc. are all security sensor applications. Test equipment such as oscilloscope, spectrum analyzer, logic analyzer, protocol analyzer, radio communication test set etc. are security sensor applications built around powerful processors. Thank to miniaturization, the test and measuring equipment are now becoming portable facilitating easy testing and measurement in the field by field-personnel.
9. **Finance**: Financial dealing through cash and cheques are now slowly paving way for transactions using smart cards and ATM (Automatic Teller Machine, also expanded as Any Time Money) machines. Smart card, of the size of a credit card, has a small micro-controller and memory; and it interacts with the smart card reader! ATM machine and acts as an electronic wallet. Smart card technology has the capability of ushering in a cashless society. Well, the list goes on. It is no exaggeration to say that eyes wherever you go, you can see, or at least feel, the work of an security sensor application.

**Challenges of security sensor application**

1. **Against Privacy Attacks: -** Attacker performs snooping through by taking same node information and easily finds the contents of communication.
2. **Traffic Analysis attacks:-**It extracts the information of content from nodes by analyzing snooping the traffic pattern on wireless communication. Example we can also find out that where the weakest spectrum zone is or where the primary users are emanating with the help of spectrum information.
3. **Impersonating Attacks:***-* It acts like the original server node and joins to the network to receive packet and analyses the traffic, using CWS features.
4. **Node Targeted Attacks:- I**t works by disrupting the nodes. It requires more attention than in a WSN because of the generation of information is important for the accurate working of CWSN. Example withdraws a cryptographic Key, changing the internal device code.
5. **Power Consumption Attacks:*-***CWSN are more vulnerable to power consumption attacks due to small size of batteries and nodes. Example access point.
6. **Policy Attacks*:-***Policy attacks are also classified into two types of attacks named as Excuse attack, Newbie Picking attack.
7. **Cryptographic Attacks:***-* The main motive of cryptographic attack is to get the cryptographic key and analyze the weaknesses in system from transmission of information. Example Differential Power Analysis Attack (DPA).
8. **Sybil attack:-**In Sybil attack, a node can act to be more than one node means a node copy the identity of other real nodes in the Sybil attack. It harms the security of data, integrity because Sybil attacks attack the distributed storage, data aggregation and routing mechanisms. Efficient Protocols are used to prevent from this attack because wireless sensor networks have base stations or gateways.

Every security sensor application consists of custom-built hardware built around a Central Processing Unit (CPU). This hardware also contains memory chips onto which the software is loaded. The software residing on the memory chip is also called the ‘firmware’. The security sensor application architecture can be represented as a layered architecture (Saravana & Paramasivan, 2016).

The operating system runs above the hardware, and the application software runs above the operating system. The same architecture is applicable to any computer including a desktop computer. However, there are significant differences. It is not compulsory to have an operating system in every security sensor application. For small appliances such as remote control units, air conditioners, toys etc., there is no need *for* an operating system and you can write only the software specific to that application. For applications involving complex processing, it is advisable to have an operating system. In such a case, you need to integrate the application software with the operating system and then transfer the entire software on to the memory chip. Once the software is transferred to the memory chip, the software will continue to run *for* a long time you don’t need to reload new software (Savoine & Menezes, 2018).

Now, let us see the details of the various building blocks of the hardware of an security sensor application. the building blocks are;

* 1. Central Processing Unit (CPU)
  2. Memory (Read-only Memory and Random Access Memory)
  3. Input Devices
  4. Output devices
  5. Communication interfaces
  6. Application-specific circuitry

**Central Processing Unit (CPU):**

The Central Processing Unit (processor, in short) can be any of the following: microcontroller, microprocessor or Digital Signal Processor (DSP). A micro-controller is a low-cost processor. Its main attraction is that on the chip itself, there will be many other components such as memory, serial communication interface, analog-to digital converter etc. So, for small applications, a micro-controller is the best choice as the number of external components required will be very less. On the other hand, microprocessors are more powerful, but you need to use many external components with them. D5P is used mainly for applications in which signal processing is involved such as audio and video processing.

**Memory**

The memory is categorized as Random Access 11emory (RAM) and Read Only Memory (ROM). The contents of the RAM will be erased if power is switched off to the chip, whereas ROM retains the contents even if the power is switched off. So, the firmware is stored in the ROM. When power is switched on, the processor reads the ROM; the program is program is executed.

**Input devices**

Unlike the desktops, the input devices to an security sensor application have very limited capability. There will be no keyboard or a mouse, and hence interacting with the security sensor application is no easy task. Many security sensor applications will have a small keypad-you press one key to give a specific command. A keypad may be used to input only the digits. Many security sensor applications used in process control do not have any input device *for* user interaction; they take inputs *from* sensors or transducers 1’fnd produce electrical signals that are in turn fed to other systems.

**Output devices**

The output devices of the security sensor applications also have very limited capability. Some security sensor applications will have a *few* Light Emitting Diodes (LEDs) *to* indicate the health status of the system modules, or *for* visual indication of alarms. A small Liquid Crystal Display (LCD) may also be used to display *some* important parameters.

**Communication interfaces**

The security sensor applications may need to, interact with other security sensor applications at they may have to transmit data to a desktop. To facilitate this, the security sensor applications are provided with Application-specific circuitry

Sensors, transducers, special processing and control circuitry may be required fat an security sensor application, depending on its application. This circuitry interacts with the processor to carry out the necessary work. The entire hardware has to be given power supply either through the 230 volts main supply or through a battery. The hardware has to designed in such a way that the power consumption is minimized.

**Programming Algorithm**

Before programming the AT89S52, the address, data, and control signals should be set up according to the “Flash Programming Modes”. To program the AT89S52, take the following steps:

* + 1. Input the desired memory location on the address lines.
    2. Input the appropriate data byte on the data lines.
    3. Activate the correct combination of control signals.
    4. Raise EA/VPP to 12V.
    5. Pulse ALE/PROG once to program a byte in the Flash array or the lock bits.

The byte write cycle is self-timed and typically takes no more than 50 µs. Repeat steps 1 through 5, changing the address and data for the entire array or until the end of the object file is reached.

**Conclusion**

The developed motion detection alarm and security system gives good response to the motion sensor when it detects intrusion at the windows or doors The test result shows that both the braking switches attached to the door hinges and the motion sensors performed adequately as expected. The entire decision making was carried out with the aid of a PICI8F2423 microcontroller. One of the main feature of the design, it is built with a time delay of 60 seconds to allow the house owner to leave before security mode is activated. This work is useful in the area of security usage, industries and in automation.

**Recommendations**

Security of persons and information has always been a major issue. We need to protect our homes and offices; and also the information we transmit and store. Developing security sensor applications for security applications is one of the most lucrative businesses nowadays. Security devices at homes, offices, airports etc. for authentication and verification are security sensor applications. Encryption devices are nearly 99 per cent of

the processors that are manufactured end up in~ security sensor applications. Security sensor applications find applications in every industrial segment- consumer electronics, transportation, avionics, biomedical engineering, manufacturing, process control and industrial automation, data communication, telecommunication, defense, security etc. Used to encrypt the data/voice being transmitted on communication links such as telephone lines. Biometric systems using fingerprint and face recognition are now being extensively used for user authentication in banking applications as well as for access control in high security buildings.

**References**

Gharaei, N., Bakar, K., Hashim, Z., Hosseingholi Pourasl, A., Siraj, M. & Darwish, T. (2017). An Energy-Efficient Mobile Sink-Based Unequal Clustering Mechanism for WSNs *Sensor*, 17(1),18-58.

Hoang, D. (2014). Real-Time Implementation of a Harmony Search Algorithm Based Clustering Protocol for Energy-Efficient Wireless Sensor Networks. *IEEE Transactions on Industrial Informatics*, 10(1),774-783.

Meena, P. & Somkuwar, A. (2014). Comparative Analysis of Information Fusion Techniques for Cooperative Spectrum Sensing in Cognitive Radio Networks. *Proceedings of International Conference on Recent Trends in* *Information, Telecommunication and Computing,* 13(1), 29-41.

Parenreng, J. & Kitagawa, A. (2017). A Model of Security Adaptation for Limited Resources in Wireless Sensor Network. *Journal of Computer and Communications*, 5(3), 10-23.

Prema, G. & Narmatha, D. (2016). Performance of Energy a Ware Cooperative Spectruim Sensing Algorithm in Cognitive Wireless Sensor Network.Online *International Conference on Green Engineering and Technologies*, 19(1), 16-27.

Saravana, A. & Paramasivan, B. (2016). Implementation of an Efficient Light Weight Security Algorithm for Energy-Constrained Wireless Sensor Nodes. *Circuits and Systems*, 7(9), 2234-2241.

Savoine, M. & Menezes, D. (2018). Andrade, Proposal of a Methodology for the Assessment of Security Levels of IoT Wireless Sensor Networks in Nuclear Environments. *World Journal of Nuclear Science and Technology,* 8(2), 78-85.

Vijayarajeswari, R., A. Rajivkannan and J. Santhosh, A. (2016). Simple Steganography Algorithm Based on Lossless Compression Technique in WSN. *Circuits and Systems*, 7(8), 1341-1351.

Wang, N., Huang, Y. & Liu, W. (2008). A Fuzzy-Based Transport Protocol for Mobile Ad Hoc Networks. *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, Taichung, 11(13), 320-325.

Zeng, B. & Yan, D. (2014). An Energy Efficient Harmony Search Based Routing Algorithm for Small-Scale Wireless Sensor Networks. *IEEE 17 the International Conference on Computational Science and Engineering*, 19(21), 362-367.