GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

Monitoring, Localizing and Securitizing of WSNs for applications in Logistics

Burla Rajesh [1] and K. Aanandha Saravanan*[2]
Vel Tech Dr. RR & Dr.SR Technical University, Chennai, TN, India
raaz.burla@gmail.com

ABSTRACT

The applications of using WSNs in logistics are presented in this paper, having some advantages (e.g., distributed processing, multi-hop routing), WSNs allow telemetry, control and management applications which can be widely used in logistics, especially in autonomous logistics systems. Originating from the requirements of future logistics systems in which the real time quality monitoring is necessary, many aspects of applying WSNs in logistics are considered, such as data collection, lifetime of sensor nodes during long transportation processes, or network management to reduce the labor work and enhance the object monitoring in logistic processes. Moreover, a context aware model based on rules helps sensor nodes to make better decisions in monitoring services. A efficient localization techniques are developed to identify positions of logistic objects. And finally the entire system is securitized by encryption method.

Keywords: WSNs in logistics, localization techniques, Encryption.

I. INTRODUCTION

The increasing demand in Wireless Sensor Networks (WSN) can be promptly, a tiny sensing material self-powered which gather information or detect special events and communicate in a wireless pattern with the end goal of handling the processed data to a base station. Its senses the information, process it and communicate through any medium. These tiny devices are capable of detecting various application fields [1], a wireless sensor network (WSN) consists of battery-operated sensor devices with computing, data processing, and communicating compo¬nents.

A sensor node is an electronic device equipped with embedded sensors, processors, radio interface and other parts such as flash, RAM, LEDs, etc. It can monitor the physical environment, process the collected data, and communicate with other nodes to transmit its data.

Most research on security in sensor networks has focused on prevention techniques, such as cryptography [3-4], key management [5-6] and authentication techniques [7-8]. Other papers study WSN attacks which were classified based on various criteria, such as the domain of the attackers, or the techniques used in attacks [9-10]. Recently, many papers are presented an overview of the different applications of the wireless sensor networks and security related issues due to the nature of these applications [11-12]. In this paper, a complete security frame work was added to the automation system implemented by using WSN in order to enhance its security defense against different types of threats and attacks. The remainder of this paper is organized as follows: section 2 includes the suggested system architecture. Section 3 explains the ciphering module of the suggested system. Section 4 explains the keys generation module of the suggested system. Section 5 includes the hardware implementation of WSN base station armed with firewall on UBICOM platform with the results. Section 6 contains an overall system evaluation and finally, section 7 provides conclusions.

1.1 Sensor node operating systems

Every sensor node needs an operating system to run its applications [2]. Operating systems for wireless sensor nodes are typically less complicated than general-purpose operating systems because of both the special requirements of sensor network applications and the resource constraints in sensor network hardware platforms.

Many operating systems for WSNs have been developed so far. Each of them is designed for a specific purpose with many features. In the following section, a brief description of some popular operating systems in WSNs is presented.

- TinyOS [3] is an open source component-based operating system and platform aiming at WSNs. This is the most popular operating system which is used widely in the sensor network community. TinyOS applications must be written in nesC, a dialect of the C language, which is optimized for the memory limitations in sensor nodes. TinyOS applications are built on components which are connected via interfaces. For easy usage, TinyOS supports components and interfaces of common abstractions, e.g. packet, routing, and storage.

- Contiki[4] is an operating system which supports loading modules over the network and supports run-time loading of standard ELF (Executable and Linkable Format) files. It is also an event-driven OS like TinyOS, but it supports multithreading on each application. Contiki configuration only consumes 2 kilobytes of RAM and 40 kilobytes of ROM.
- SOS [5] is also an event-driven operating system like TinyOS and Contiki. The primary feature of SOS is its support for loadable modules. The main feature of SOS is that a complete system is built from smaller modules, which can be possibly loaded at run-time.

Among these operating systems, TinyOS is widely supported by a large sensor networks community because TinyOS has several advanced features such as simple programming, low footprint, and it is designed towards industrial solutions. Hence, TinyOS is chosen to be incorporated with the sensor nodes in this paper.

1.2 Applications of WSNs

A WSN is a set of sensor nodes, which collaborate to perform the task of collecting data in an area and sending them to the target destination through wireless networks. WSNs encourage many novel and existing applications such as [6]:

- General engineering: automotive telemetry, smart house, tracking items, wearable computing
- Monitoring: environmental monitoring, disaster detection
- Civil engineering: monitoring of structures, disaster recovery
- Health monitoring: medical sensing Military monitoring: asset monitoring, surveillance and battle-space monitoring.

Nowadays, with their rapid development, Wireless Sensor Networks (WSNs) have gone beyond the scope of monitoring the environment to become part of the Internet of things [7]. The next subsections present the application of WSNs in logistics and the advantages.

1.3 Requirements in logistics

Many research activities have the goal to improve the quality of logistics systems. However, there are some key issues in logistics optimization as follows:

- The information of all logistic objects has to be accurate, timely, and comprehensive. This requires an advanced technology, which allows the system to observe the data of objects and report them timely.
- Integration is another important factor, which should be considered for optimization because a logistics system consists of many smaller entities and processes. The integration can help to synchronize data in all parts of the whole system efficiently.
- Because there are potentially many solutions for a logistic problem, the best solution is the solution that meets the requirements in a reasonable amount of time. With thousands of information sources, distributed processing is a suitable way to let each object process its own information and the centralized management gathers this filtered information to be able to make strategic decisions.

Last but not least, another issue is the fact that the intelligent logistics system requires not only the passive information of the goods but also every condition of the surroundings related to them. Reporting unexpected events happening to the goods in transportation is indeed necessary in modern logistics.

II. APPLICATIONS OF WSNs IN LOGISTICS

For the use in logistics, the current low-cost nodes with embedded sensors (e.g., temperature, humidity, and pressure sensors) can be programmed to perform specific tasks [8]. They can monitor the condition of goods in transport vehicles and report the status to the data center (centralized or distributed) during the transportation time from the departure location to the destination. Problems or activities which can be detected by sensors and are happening to the goods on the way will be reported via available distributed networks to which the transport vehicle can be connected (e.g., UMTS/GPRS, WLAN, WiMax).

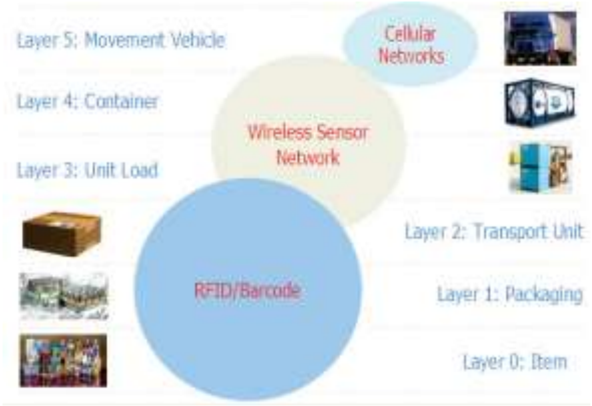

Figure: 1 Technologies used in logistics

Applications of WSNs can be extended to monitoring the surroundings such as sensors in warehouses, trucks, containers, and on ships, etc. In these applications, sensor nodes are tagged on facilities to form a self-organized network and report the environmental conditions inside warehouses for alerts or management. **Figure.1** shows the layers in logistics and the technologies that can be used correspondingly.

2.1. Mapping of logistic objects

The philosophy of applying WSNs in logistics is that if a physical logistic object is completely mapped into an information object, the management of the information object flow can replace the management of the physical object flow [9]. Moreover, thanks to information technologies, the management of information objects is much more convenient and easier than physical logistic ones due to a variety of management tools available.

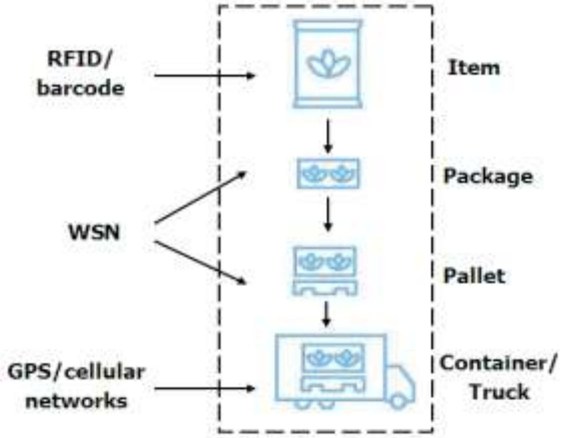

Figure.2 Object mapping

In **Figure.2**, a mapping of logistic objects is shown in three reduced levels:

- Items are equipped with a barcode or an RFID that contains passive information used to identify the item. This information can be used to recognize the type of products, the size, or weight of products. However, these technologies cannot provide the real time information of products such as the temperature around the items, which changes due to the external physical environment.
- Package/Pallet uses WSNs to report the environmental conditions inside. These objects can communicate with each other using multi-hop routing protocols for data transmission. The self-organizing feature of WSNs supports the dynamics of logistic objects.
- A container or a vehicle uses a gateway to bridge the collected data between the WSNs/RFID and an available cellular network (e.g., UMTS, GPRS) it can connect to. The monitoring data is transmitted to the data center for management or making decisions. GPS is also used in vehicles to track their position in real time.

The integration of WSNs in logistic items can provide a promising solution for monitoring the quality of goods and help to improve the flow of management processes based on the more detailed information of goods which is provided by WSNs.

2.2. Application category

Based on the characteristics of their operations, applications of WSNs are categorized in two classes: tasking and query.

i. Tasking application

A tasking application involves programming sensor nodes to perform a specific sequence of actions when nodes detect the occurrence of predefined events. Events can be the trigger signals of hardware modules inside a sensor node such as the ADC (Analog-to-Digital Converter) or the radio chip. They can also be the changes of physical environment or data packets from neighbor nodes. A task can be as simple as independently reporting a sensing value from a sensor to the gateway, but it may as well be a complex collaboration between nodes to achieve a higher accuracy [10]. For example, in a distributed localization process, nodes have to exchange their estimates to neighbors so that the localization error is lower.

In case a sensor node has both sensors and actuators, the tasking application can process information collected from sensors. After optimizing the data, the actuators can be controlled to affect the physical environment. An example of this scenario is controlling air conditioners in the rooms of a warehouse based on the collected temperature readings from sensors deployed in each room.

ii. Query application

A query application is used for request and reply packets in networks. In this mode of operation, a sensor node only replies with a data packet when it receives a request from the observers.

A query can be as simple as obtaining raw data from one sensor node. However, in some situations, a more complicated query is needed. For example, a query such as “which packet (embedded with sensors) inside the container has the highest humidity” requires a data collection [11], filtering, and aggregation between sensor nodes in the network.

Queries provide a means to get the network status such as topology or link quality for management. In addition, information about the node status (e.g., remaining battery, operation mode) can also be collected by queries.

III. LOCALIZATION TECHNIQUE

Localization is an important feature of logistics systems, especially in case the advanced logistic objects are introduced by applying sensor nodes in objects. A localization technique based on signal strength is proposed and examined in both cases: determining the relative positions (in a pre-defined coordinate) of containers in a free-space environment and identifying the package positions inside the container with complicated signal attenuation conditions in various environments. This service utilizes the signal strength collected by the neighbor exchange protocol [12]l. The results are investigated in both simulations and experiments to estimate the relative locations of sensor nodes in a pre-defined coordinate system, which show a good result when using this localization technique in free space environment such as indentifying a container in a harbor. However, this localization technique is not accurate enough in all investigated scenarios.

3.1 Common localization techniques

Received Signal Strength Indicator (RSSI) -based schemes are considered in this work because RSSI is a value which is available in many sensor hardware platforms and it is believed to be a good indicator for distance[13]. Generally, localization algorithms assume the presence of a limited number of reference nodes in the network, which are called beacon nodes or anchor nodes.

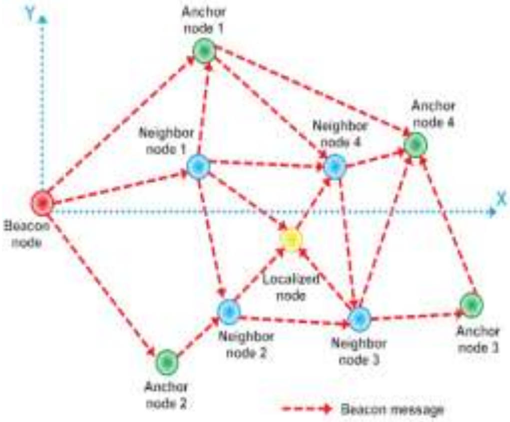

Figure.3 Definitions of node types and relative coordinates

In order to have a clear description, **Figure.3** illustrates the definitions of node types as used in this thesis as follows:

- An anchor node is a node which knows its location or its coordinates, and is used as a reference point for the other nodes to compute their locations. The advantage of using anchor nodes is the simplification of the task of assigning coordinates to the other nodes.
- A beacon node is also an anchor node, which additionally generates and broadcasts beacon messages to the network[14]. In the given example, beacon and anchor nodes are not the same because an anchor node does not necessarily create beacon messages. In the general case, all the node positions are equally shifted so that the beacon node is the centre of this relative

coordinate. Therefore, for simplicity, the beacon node is assumed to be located at the origin of the local (or relative) coordinate system. Here, the routing protocol controlled by the beacon node is used to carry the localization information.

A localized node is a node which performs the localization algorithm [15]. Hence, in order to be able to perform the location estimation, a network can have one beacon node, several anchor nodes and localized nodes or have only beacon nodes and localized nodes because beacon nodes can act as anchor nodes.

The following section describes two common categories of RSSI-based schemes, i.e. range-based and range-free localization.

Range-based algorithms use RSSI to estimate the position of a specific node by measuring the distances between nodes. There are many techniques classified into this category. Min-Max is a very popular localization algorithm because of its simple implementation. The key idea is to build a bounding box for each neighbor node using its distance and its estimate. Then, the localized node determines the intersection box of these boxes. The centre of the intersection box is the estimated location of the localized node (shown in **Figure.4**).

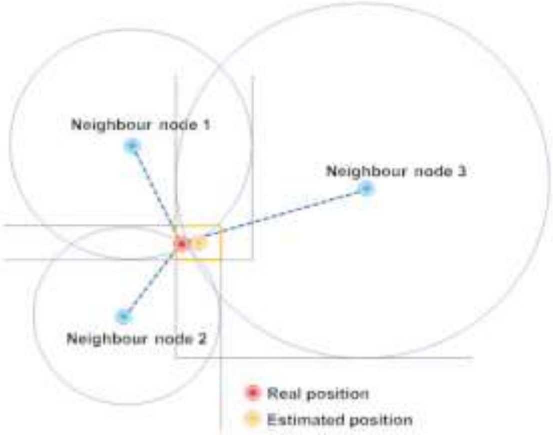

Figure.4 Min-Max algorithm.

Triangulation is a simple range-based, distributed localization method based on geometric properties. The localized node collects the beacon messages and estimates the distances to neighbor nodes. Next, it builds the circles for neighbor nodes by using the calculated distances, which is shown in **Figure.5**. The intersection of these circles is the estimated position of itself. However, this technique is more complicated to be implemented because solving a system of 3 equations is a computational challenge for resource-limited devices

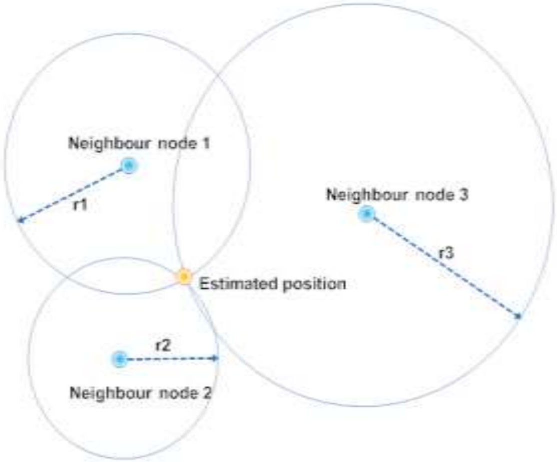

Figure.5 Triangulation algorithm

Weighted Centroid Localization (WCL) is also a distributed method coming from the idea of using the distances between the localized node and neighbor nodes as weighted coefficients (shown in **Figure.6**). These coefficients are determined from a propagation model [16]. However, the localization error of range-based schemes is usually affected by radio propagation behaviors, especially in indoor environments. Other important factors that also have influence on the localization accuracy are the number of anchor nodes and their positions.

In RSSI-based range-free algorithms, RSSI is used to map the locations in an area instead of measuring the distances between localized node and neighbor ones. MoteTrack performs accurate measurements of RSSI values in an area of interest to build a signal strength map. The localized node receives the beacon messages from its neighbor nodes and compares them with a pre-built RSSI map in the database to get its location. These schemes can achieve a very high accuracy but they require an off-line measurement from operators. Moreover, if there are any changes in that area, the process of building the signal strength map has to be done again.

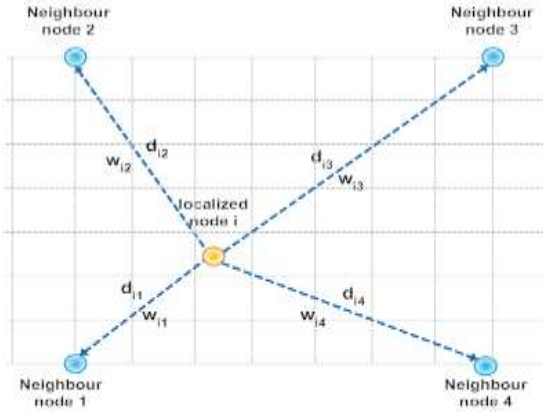

Figure.6 WCL algorithm

3.2 Results and Discussion:

Formulation for WCL algorithm**:**

$$P_i^{\text{estimate}} (x, y, z) = \frac{\sum_{j=1}^{n} \text{W i,j.Pj neighbor (x,y,z))}}{\sum_{j=1}^{n} Wi,j} \quad \text{------ (1)}$$

$$Wi,j= 1/(d_{i,j})^g \quad \text{---------------(2)}$$

in which:

- *wi,j*: coefficient from sensor node *i* to neighbor node *j*, depending only on the distance between them
- *g*: degree, usually depends on propagation model.

This algorithm gains a higher accuracy because it considers the distance as a parameter for localization. However, due to the limited resources in embedded devices, the calculation of *wi,j* is not easy.

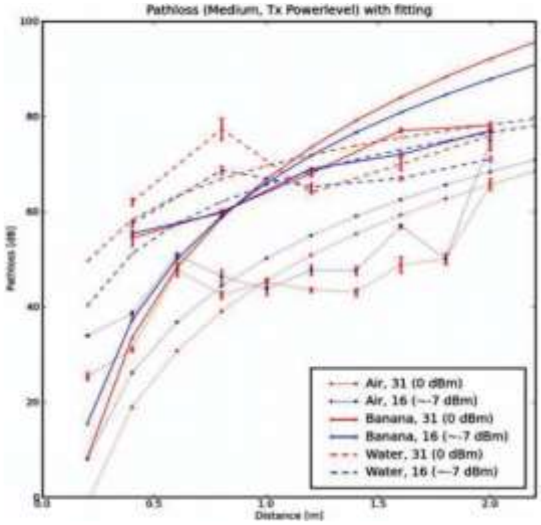

Figure.7 Radio propagation model in some environments

To apply the use of this algorithm in logistics applications, **Figure.7** WCL is considered whether it can be efficient or not when it is implemented inside containers which have complicated signal propagation conditions. Based on research work of, a fully-loaded banana container is taken into account in this part. Figure shows the path loss of a radio signal in several environments. One can see from this figure that if the sensitivity threshold of a sensor node is -90 dBm , nodes cannot successfully receive data at distances over 2m.

3.3 Refinement by exchanging position information

The goal of this phase is to refine the node positions calculated in the previous phase. These positions are not accurate because not all of the available information is used in the first two phases. This phase makes the estimated position of a node converge to the real position as close as possible. In the logistic environment, the mobility of objects is very important. Hence, the location parameters are continuously calculated over time. Of course, the beacon node and the anchor nodes do not perform the refinement because they know their positions.

Figure.8 shows an example of the refinement phase of a sensor node running the localization process. It can be seen that the estimated location will converge to the real location over time in the local coordinate. It can be noted that the local coordinate only expresses the relative distance between a localized node position and the beacon node position.

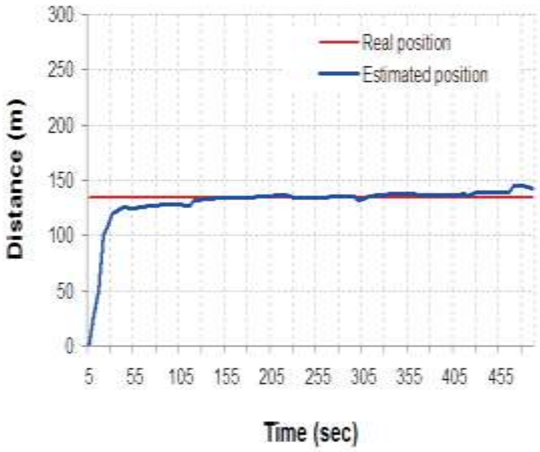

Figure.8 The estimation over time in localization process of a static node

IV. SECURED DATA TRANSMISSION

Because WSNs use the wireless environment for transmission, they are vulnerable to attacks, which are more difficult to carry out in wired communications. Hence, the wireless environments are difficult to protect due to the broadcast medium. In this section, the security issues are discussed to allow secured data transmission in WSNs.

4.1 Security in link layer

In some radio hardware platforms, the security at link layer is supported as an in-line feature. It supports Message Authentication Codes security operations, which can be viewed as a cryptographically secure checksum of a message. All security operation uses AES encryption with 128-bit keys within transmit and receive FIFOs on a frame basis. In addition, a stand-alone AES encryption can be also used to encrypt a 128-bit plaintext to a 128-bit cipher text.

4.2 Public key cryptography

At the application layer, a data packet can be encrypted before it is transmitted. In secured transmission mode, a public key cryptography (PKC) mechanism can be used to secure the transmitted data of each sensor node [17].

Public key cryptography is based on asymmetric algorithms with two different keys which are called public key and private key:

- The public key is known to every sender in the network. Each sender node uses this key to encrypt its data messages.
- The private key is only kept by the receiver to decrypt a received message from a sender.
- The relation between a public key and a private key is defined by a mathematic function so that it is easy to create a public key from a given private key but it is very hard to create the private key from a public key.

The advantage of public key cryptography is that it is not necessary to transmit keys between the sender and the receiver; hence, the communication is more secured. Moreover, the encryption and decryption uses the same algorithm at the sender and the receiver with different keys [18].

4.3 Encryption and decryption in WSNs

Applying encryption and decryption using PKC in WSNs requires that nodes have their own public keys. These keys can be the same or different due to the configuration from users. Each originating sensor node uses a public key to encrypt its originated data message before transmitting it to the wireless medium. Because nodes only do the encryption without decryption and some information in the packet header can be used by intermediate nodes (e.g., TTL or hop count), only the sensor readings field of a data packet should be encrypted. Moreover, the applying of PKC does not affect the self-configuration feature of WSNs because nodes do not use this information for its operation such as joining or leaving a network [19]. The data are also transmitted with the encryption provided by PKC mechanism. At the sink, with the private key of each corresponding sensor node, the sink can decrypt the data message without knowing the public keys of the sending nodes. If the data collection is assigned to another sink due to the sink failures for example, the database of private keys needs to be synchronized by a synchronization protocol. Otherwise, the new sink has to reinitialize the key assignment to all nodes in network for data collection.

The progress of encryption and decryption is shown in Figure 9, in which the Manager (the sink) is the software WSN data Collection and Management System that can collect the messages and decrypt them. However, the data flow from the sink node to the network (control data) should not be secured by PKC because the decryption takes many resources while sensor nodes are resource-limited [20]; hence this process should be done at the sink. Additionally, false commands cannot be sent if the user does not have the authentication with the Manager software (shown in **Figure.9**).

In the implementation of the proposed design in this thesis, the reading value of each sensor node is scrambled by a 16-bit key and the descrambling process is carried out by WSN data Collection and Management System when it successfully receives the packet. However, any advanced encryption such as TinyECC can be implemented as discussed above.

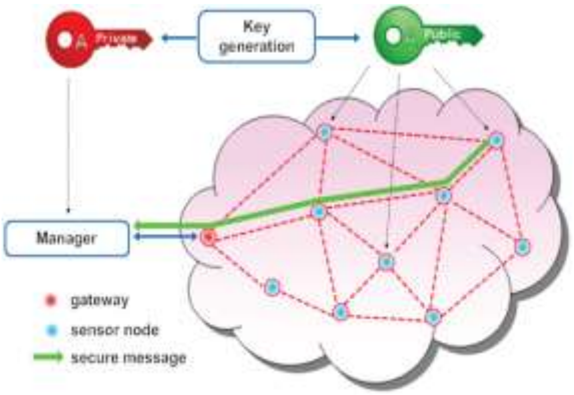

Figure.9 Data security in WSNs using public-key cryptography

V. CONCLUSIONS

In this paper, a general application model is proposed and discussed in the WSN domain with many issues from sensing tasks to memory utilization. This model supports many kinds of sensing applications (automatic data transmission, query-based transmission, and context-aware application). The management services of sensor nodes are also considered in this part, which allow users to control or optimize the network performance. In addition, an RSSI-based localization technique, namely WCL, is integrated as a service of the application in nodes. Finally, all concrete modules are integrated in one unique system which can support the operation of sensor nodes better and make them smarter. This system can be used not only in logistic applications but also in many other areas such as monitoring applications.

VI. REFERENCES

[1] V.Q. Son, B.L. Wenning, A. Timm-Giel, C. Görg. A model of Wireless Sensor Networks using Context-awareness in Logistics Applications. In the Proceedings of the 9th Conference on Intelligence Transportations Systems Telecommunications (ITST), pp. 2-7, Lille, France, October 2009.

[2] V.Q. Son, B.L. Wenning, A. Timm-Giel, C. Görg. Enhanced Intelligence of Wireless Sensor and Actuator Networks in logistics by applications of context. In the Proceedings of the International Conference on Logistics and Maritime System (LOGMS2010), pp. 563-571, Busan, Korea, September 2010.

[3] V.Q. Son, B.L. Wenning, A. Timm-Giel, C. Görg. WiSeCoMaSys: a Tool for Data Collection and Management of Wireless Sensor Networks. In the Proceedings of the International Conference on Advanced Technologies for Communication (ATC2010), pp. 43-48, Ho Chi Minh City, Vietnam, October 2010.

[4] I. Talzi, A. Hasler, S. Gruber, C. Tschudin. PermaSense: Investigating Permafrost with a WSN in the Swiss Alps. In Proceedings of the Fourth Workshop on Embedded Networked Sensors, pp. 8-12, Cork, Ireland, June 2007.

[5] Locating Assets: Technology Choices, available at http://www.terahop.com/docs/Location%20Technologies%20THN%2 0AN-003.pdf, last access in April 2011.

[6] TeraHop Movable Wireless Sensor Networks and RFID Integration: A General Discussion, available at http://www.terahop.com/docs/RFID%20IntegrationTHN%20AN- 002_JED.pdf, last access in April 2011.

[7] A.Timm-Giel, K. Kuladinithi, M. Becker, C. Görg. Wireless Sensor Networks in Wearable and Logistic Application. In CRUISE Workshop, Greece, June, 2006.

[8] TinyOS Website, available at http://www.tinyos.net, last access in April 2011.

[9] Getting Data from Tmote Sky’s Sensors, available at”http://docs.tinyos.net/index.php/Boomerang_ADC_Example”, last access in April 2011.

[10] M. Turon. MOTE-VIEW: A Sensor Network Monitoring and Management Tool. In Proceedings of

the Second IEEE Workshop on Embedded Networked Sensors (EmNetS-II), pp. 11-18, Sydney Australia, May 2005.

[11] United Parcel Service (UPS), available at http://www.ups.com, last access in April 2011.

[12] VeriSign Inc., available at http://www.verisign.com, last access in April 2011.

[13] Virtual Router Redundancy Protocol, available at http://www.cisco.com/en/US/products/hw/vpndevc/ps 2284/products_t ech_note09186a0080094490.shtml, last access in April 2011.

[14] M. Wachs, J. I. Choi, J. W. Lee, K. Srinivasan, Z. Chen, M. Jain, P. Levis. Visibility: A New Metric for Protocol Design. In Proceedings of the Fifth ACM Conference on Embedded Networked Sensor Systems (SenSys), pp. 73–86, Sydney, Australia, 2007.

[15] B. Warneke, M. Last, B. Liebowitz, KSJ. Pister. Smart dust: Communicating with a cubic-millimeter computer. IEEE Computer Magazine, 2001, Volume 34, Issue 1, pp. 44-51.

[16] G. Werner-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J Lees, M. Welsh. Deploying a Wireless Sensor Network on an Active Volcano. IEEE Internet Computing, Volume 10, Issue 2, pp. 18-25, March 2006.

[17] B.-L. Wenning, A. Lukosius, A. Timm-Giel, C. Görg, S. Tomic. Opportunistic Distance-Aware Routing in Multi-Sink Mobile Wireless Sensor Networks. In Proceedings of ICT-MobileSummit 2008, CDROM publication, Stockholm, 2008.

[18] B.-L. Wenning, D. Pesch, A. Timm-Giel, C. Görg. Environmental Monitoring Aware Routing in Wireless Sensor Networks. In Proceedings of the IFIP International Federation for Information Processing, Volume 284/2008, pp. 5-16, Toulouse, France, September 2008.

[19] A. Warrier, I. Rhee. Stochastic analysis of wireless sensor network MAC protocols. In Technical report, Computer Science Department, North Carolina State University, Raleigh, NC, 2005.

[20] A comparison of Radio Frequency Identification Technologies and Terahop Movable Wireless Sensor Networks, available at http://www.terahop.com/docs/RFID%20Comparisons %20THN%20A N-001_JED.pdf, last access in April 2011.