Circuits and Systems, 2016, 7, 2234-2241
Published Online July 2016 in SciRes. http://www.scirp.org/journal/cs
http://dx.doi.org/10.4236/cs.2016.79194

Implementation of an Efficient Light Weight Security Algorithm for Energy-Constrained Wireless Sensor Nodes

A. Saravanaselvan[1], B. Paramasivan[2]

[1]Department of ECE, National Engineering College, Kovilpatti, India
[2]Department of CSE, National Engineering College, Kovilpatti, India
Email: asselvan1981@gmail.com, bparamasivan@yahoo.co.in

Received 27 April 2016; accepted 4 May 2016; published 18 July 2016

Abstract

In-network data aggregation is severely affected due to information in transmits attack. This is an important problem since wireless sensor networks (WSN) are highly vulnerable to node compromises due to this attack. As a result, large error in the aggregate computed at the base station due to false sub aggregate values contributed by compromised nodes. When falsified event messages forwarded through intermediate nodes lead to wastage of their limited energy too. Since wireless sensor nodes are battery operated, it has low computational power and energy. In view of this, the algorithms designed for wireless sensor nodes should be such that, they extend the lifetime, use less computation and enhance security so as to enhance the network life time. This article presents Vernam Cipher cryptographic technique based data compression algorithm using huff man source coding scheme in order to enhance security and lifetime of the energy constrained wireless sensor nodes. In addition, this scheme is evaluated by using different processor based sensor node implementations and the results are compared against to other existing schemes. In particular, we present a secure light weight algorithm for the wireless sensor nodes which are consuming less energy for its operation. Using this, the entropy improvement is achieved to a greater extend.

Keywords

In-Network Data Aggregation, Security Attacks, Vernam Cipher Cryptographic Technique, Huffman Source Coding, Entropy

How to cite this paper: Saravanaselvan, A. and Paramasivan, B. (2016) Implementation of an Efficient Light Weight Security Algorithm for Energy-Constrained Wireless Sensor Nodes. *Circuits and Systems*, **7**, 2234-2241.
http://dx.doi.org/10.4236/cs.2016.79194

1. Introduction

A sensor network is made up of several sensor nodes containing processing element, sensors, wireless transceiver and a small battery. Communications are typically based on the IEEE 802.15.4 standard due to its limited battery life. Sensor nodes are to have several critical requirements like energy consumption, processing capability, low memory capacity and less cost. The main challenge in WSNs is reducing the power consumption of the energy constrained sensor nodes. A typical strategy is used for reducing the transmission of data among the sensor nodes. Thus, an additional intelligent layer is required for compressing the data transmissions and receptions.

Efficient kind of source coding techniques can be used to compress the data and in turn reduces the number of data to be transferred. Variable length coding is used to improving the entropy efficiency and improves the energy consumption of the sensor nodes. This algorithm assigns different number of binary digits to the sensed data according to their probabilities of occurrence. In order to extend the lifetime of WSNs, no local data processing is performed on sensor nodes and sensed data is transmitted to the base station for further processing. But, this strategy consumes a more communication energy because of the large amount of data being transmitted from sensor node to base station. In order to minimize the data transmission rate from sensor node to base station, source encoding scheme is preferred. In addition, security schemes consist of processes which ensure confidentiality, integrity and authentication of the information being transmitted over wireless medium against to the security related attacks injected purposefully from node-to-node communication.

Typically, a sensor node is highly constrained due to computation capability and energy resources. In large WSNs, computing aggregates reduce the amount of communication and energy consumption. Rapid development of system miniaturization, wireless communication and on-chip signal processing enhances the development of wireless sensor technology [1] [2]. However attack resilient and energy consumption still remains as a major problem for the full deployment and exploitation of this technology. The major challenge in WSNs is reducing the size of sensors, processing power and memory storage. To address the critical security issues in wireless sensor networks, the research community uses cryptographic and authentication techniques.

Security is a major term which comprises of data Confidentiality, Integrity, Availability and Authentication. For the secure transmission over variety of attacks several cryptographic techniques can be used. The encryption-decryption techniques used for the traditional wired networks are not suitable to be applied directly for the wireless sensor networks. Applying any kind of encryption scheme needs transmission of additional bits and hence more processing, memory and battery power which are very important for lifetime improvement of sensors. In addition, applying the security mechanism could also increase delay, jitter and packet loss in WSNs.

Wireless networks are more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. The life time can be estimated with duty cycle, network coding and combinations of duty cycle and network coding. The per node energy consumption in case of a WSN with low duty cycle is more than a WSN with low duty cycle and network coding [3]. A better tradeoff between the communication overhead and security properties can be provided in order to enhance security and lifetime proportionally with suitable algorithms implementation [4]. Cluster based multi hop routing to be considered as energy efficient routing scheme for WSN. To withstand the vulnerabilities security services such as authentication, confidentiality and data integrity need to be maintained in the sensor network. Suitable techniques present solutions to prevent injection of false data in a network and defend against data compromisation [5].

Event oriented data aggregation technique uses node membership model to aggregate the information of events in sensor networks. This event oriented data aggregation decreases the energy consumption of data delivering and fulfil the application target of event detection. But, this approach does not consider the security measures [6]. The employment of cluster head for data collection elevates a new security challenge. An attacker tries to capturing keys from a number of deployed nodes and hence gains control of the network [7]. Traditional schemes using asymmetric key cryptography based schemes are expensive due to their storage and computation cost [7]. The multi cluster structure helps to minimize the broadcast overhead compared to the local structures approach with certain geocast regions that yields huge broadcast rounds overhead [8]. Wireless sensor networks are building upon an open medium that makes it easy for adversaries to inject security attacks [9].

The selection of the cryptographic techniques depends on the processing ability of wireless sensor nodes present in sensor networks and the security mechanisms are highly application specific. Moreover, sensor nodes are characterized by the constraints on energy, computation capability, and memory and communication bandwidth. The design of security services in WSNs must satisfy these constraints [10]. Security is a major issue for protocol designers due to sensor node constraints in WSN applications [9] [11]. Each node evaluates trustworthiness of its neighbour nodes behaviour by verifying the neighbour nodes identity. This kind of trust model is severely energy constrained and needs low power consumption [12] [13]. The traffic analysis examines the length of message, pattern of the message and time field. All security solutions proposed for sensor networks need to operate with minimum energy usage with low cost [14] [15].

Motivating this, it is proposed to implement a light weight security algorithm on sensor node design along with source coding scheme to enhance security and lifetime of sensor nodes. The remainder of this paper is organized as follows. Section 2 deals the proposed system model and algorithm for sensor node implementation. Section 3 discusses energy issues while performing packet transmissions and receptions by the sensor nodes. Section 4 analyzes the performance of the proposed system model with other existing schemes. The conclusion is finally drawn in Section 5.

2. System Model

In the proposed scheme shown in **Figure 1** contains X authorized nodes and Y attack nodes are deployed in a target area within the transmission range under the cluster head control. The authorized nodes used to sense the toxic gases from the target area. Attack nodes are designed in such a way that to monitor the information send by the authenticated node(s) and modify its content.

The processor based microcontroller is chosen as the processing element and it is programmed to implement the algorithm shown in **Figure 2**.

NMC—Node Membership Certificate;

The corresponding algorithm is given in Algorithm 1.

Algorithm 1:

```
1. Configure on-chip UART of microcontroller with CC2500 RF module.
2. NMC = {Unique Node-ID, Unique Signature}.
3. Distribute NMC to Sensor Nodes.
4. Receive frame from Sensor Node.
5. If (Node ID & Sign are correct)
Accept the frame else Reject the frame.
6. Decrypt the reduced payload data after compression.
7. Recover the actual payload data.
8. Issue necessary control commands to consent Node.
```

To provide a security solution, all the sensor nodes in the network assigned with Node Membership Certificate (NMC) and this certificate is issued only by the cluster head. The format of the cluster head data packet includes node ID and NMC sign. Each node in the network receives NMC and verifies its node ID and signature. Once this verification is done successfully, then the node sends back the status information. The format of the data packet includes: Unique node-ID, Payload, Unique signature and Time stamp fields. The Max payload

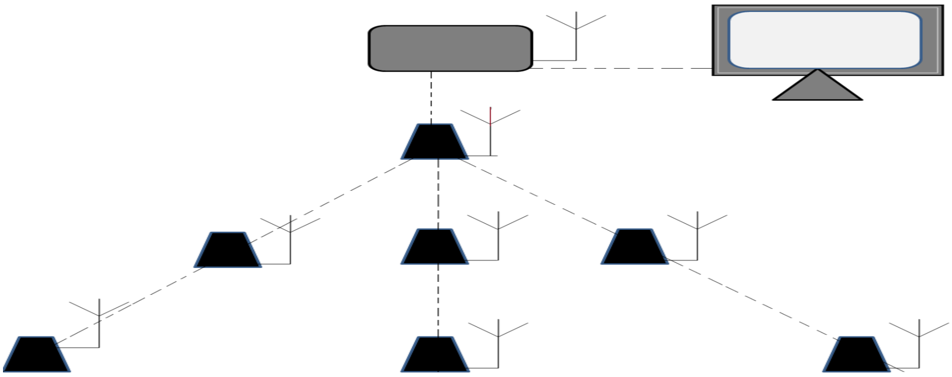

Figure 1. Hardware schematic diagram of proposed network.

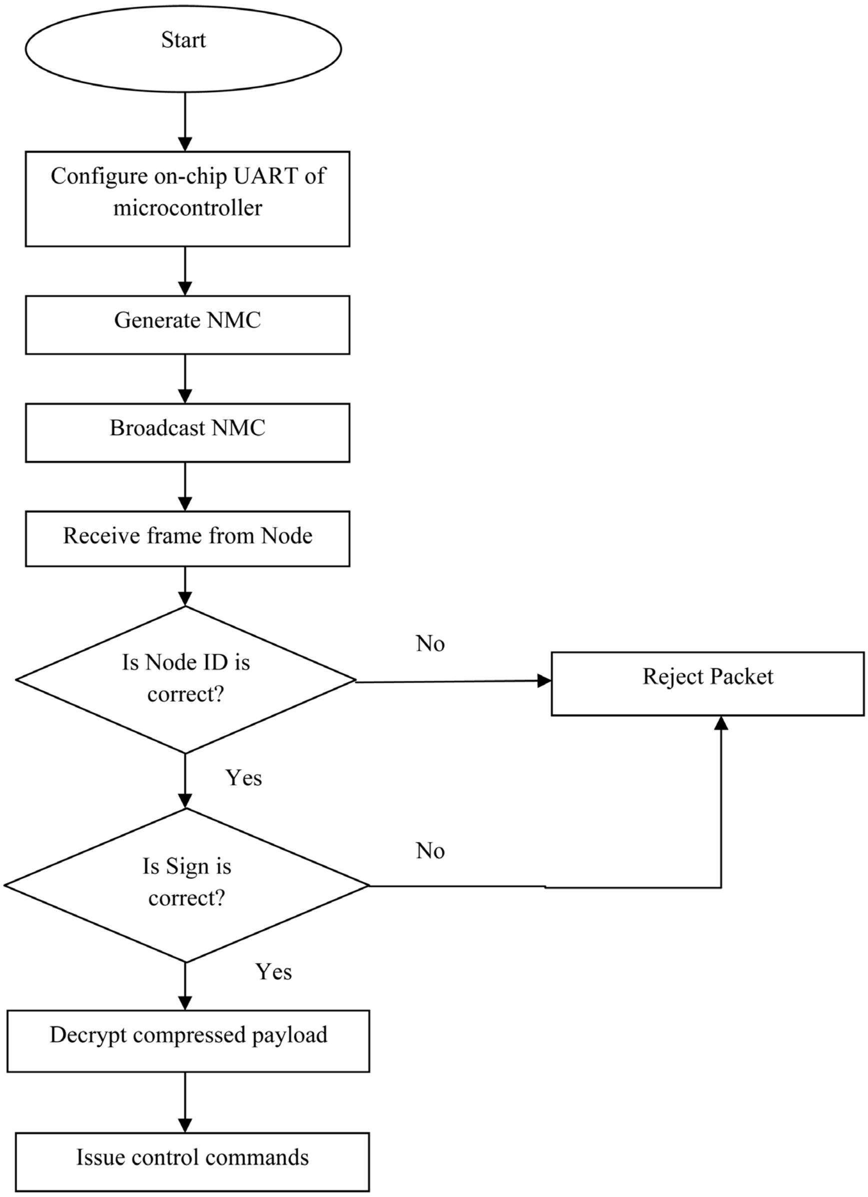

Figure 2. Flow chart for NMC generator and Vernam decryption (cluster head).

length is restricted to "X" byte long and depending upon the selected type of application, the size of "X" can be determined. In that scheme, the actual data to be transmitted contains 5 fragments and each segment length is 4, 8, 12, 16 and 20 bytes respectively. The actual payload of the sensed information is compressed using Huffman source encoding scheme and thus compressed payload has obtained. Then, the compressed payload is encrypted using Vernam cipher technique. The most significant point here is that once this time pad of Vernam cipher is used, it is never used again for any other message. The length of the encrypted payload is equal to the length of the compressed payload. The NMC verification and encryption logic is shown in **Figure 3**.

The corresponding proposed algorithm is given in Algorithm 2.

Algorithm 2:

1. Configure on-chip UART of microcontroller unit with CC2500 RF module.
2. Receive NMC.
3. If (Node-ID == consent Node)
4. Register Node ID; else retransmit Node ID to neighbourhood Node.

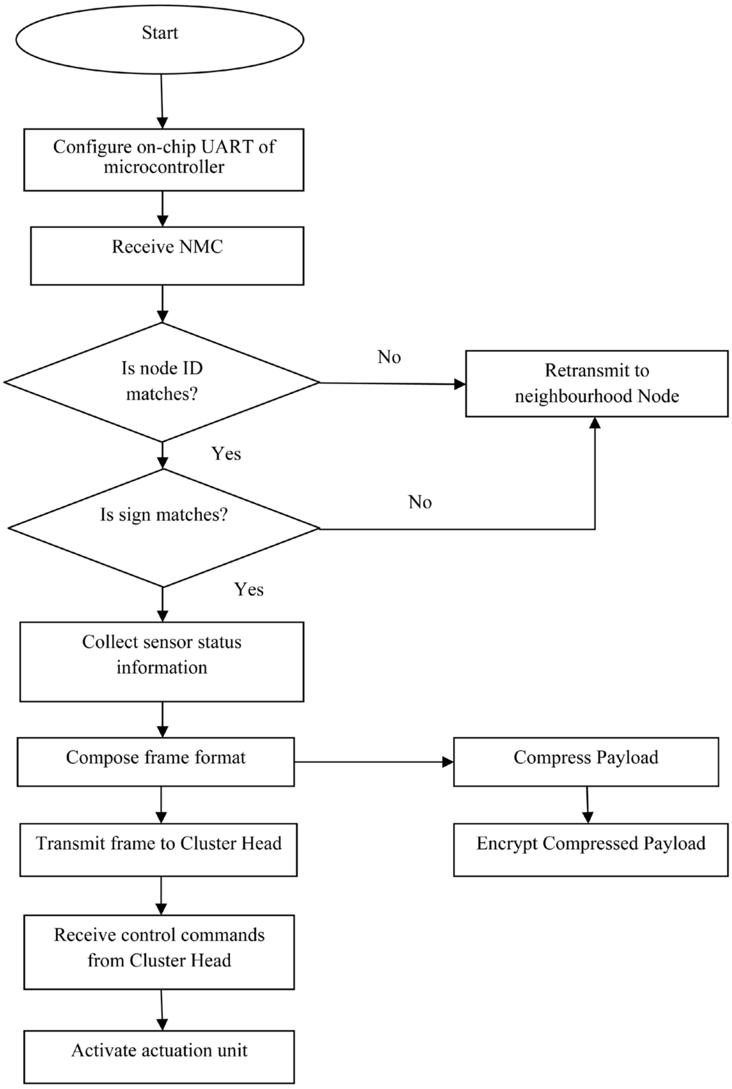
Start
Configure on-chip UART of microcontroller
Receive NMC
Is node ID matches?
No
Retransmit to neighbourhood Node
Yes
Is sign matches?
No
Yes
Collect sensor status information
Compose frame format
Compress Payload
Transmit frame to Cluster Head
Encrypt Compressed Payload
Receive control commands from Cluster Head
Activate actuation unit

Figure 3. Flowchart for NMC verifier and Vernam encryption (sensor node).

5. Register Node-Sign; else retransmit Node ID to neighbourhood Node.
6. Sense the Sensor information and store it.
7. Compress the payload data and apply Huffman source encoding.
8. Encrypt compress payload data.
9. Compose frame as {Node-ID, Payload, Sign}
10. Transmit the frame via RF module.

3. Energy Issues

The energy consumed by a communication device is more during transmission and reception. One important contribution to reduce power consumption of sensor node components comes from chip level and lower technologies. Designing low power chips is the best starting point for an energy efficient sensor node design. In principle, the energy consumed by a transmitter is due to two sources: One part is due to RF signal generation which mostly depends on chosen modulation and target distance and hence on the transmission power P_{tx}, that is power radiated by the antenna. A second part is due to electronic components necessary for frequency synthesis, frequency conversion and filters. The transmitted power is generated by the amplifier of a transmitter. Its own power consumption P_{amp} depends on its architecture but for most of them their consumed power depends on the power they are to generate. A more realistic model assumes that a certain constant power level is always required irrespective of radiated power.

After sensing the parameters the results should be transmitted to the base station via other intermediate nodes. If the two sensor nodes to communicate, the energy consumption needed for data transmission can be expressed as

$$E_{Tx} = E_{e\_tx} \cdot k + \varepsilon_{amp} \cdot d^{\gamma} \tag{1}$$

where k is the number of transmitted data bits; γ is a path loss exponent valued from 1 to 5, depending on the environment of wireless transmission; d is the distance between two sensor nodes; ε_{amp} is the amplification co-efficient to satisfy a minimum bit error rate to ensure reliable reception of the receiver; E_{e_tx} is the dissipated energy to operate the transceiver which is expressed as

$$E_{e\_tx} = V_{DD} \cdot I_t / k_{rate} \tag{2}$$

where V_{DD} is the operating voltage; I_t is the operating current; k_{rate} is the data transmission rate. During the reception, receiver circuitry has to be powered up, requiring energy of E_{e_tx}.

The energy consumed for receiving a data stream is expressed as

$$E_{ex} = E_{e\_rx} \cdot k \tag{3}$$

For a fixed distance, E_{e_rx} is constant one; so the energy consumed is proportional to the number of data bits is to be transmitted. As per the topology considered in **Figure 1**, each sensor node transmits its own frame to the base station through other intermediate nodes. Since the payload is reduced one, the energy consumption in this case is calculated as

$$E_t = \sum\nolimits_{n=1}^{N} \left[\left(E_{e_{tx}} + \varepsilon_{amp} \cdot d_n^{\gamma} \right) \cdot k_t \right] \tag{4}$$

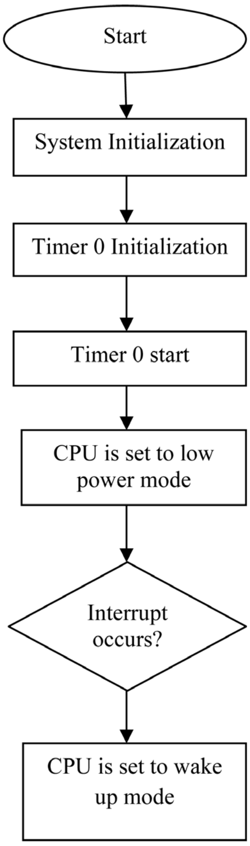

Figure 4. Sleep and active mode scheme of sensor node.

where N is the number of sensors; d_n is the distance between two sensor nodes; k_t is number of data bits of reduced payload. To minimize the node level energy, it is planned to adopt the periodic sleep and active mode operation of the proposed scheme is shown in **Figure 4**.

4. Results and Discussion

To evaluate the performance of the proposed scheme, modern processor based sensor nodes were used and the proposed scheme run on different sensor nodes. In addition, the embedded C code for RSA+SHA-1 and ECC + SHA-1 were executed on different microcontroller based sensor nodes in order to compare the execution cycle count of our proposed scheme and the results are shown in **Table 1**. To do this, speed analyzer tool of Keil IDE and IR work bench IDE were used.

Since the proposed scheme has less computations when compared to above existing schemes, the number of cycles required for execution of the proposed algorithm is lower than other two schemes. From **Table 1**, it is inferred that the proposed scheme implementation on ATMega 128 microcontroller based sensor node consumes less execution cycles when compared to other implementation due to its process technology. So that, the energy consumption analysis is being carried out for ATmega 128 microcontroller based sensor node implementation using power analyzer tool in IR work bench IDE software tool and the results are shown in **Table 2**.

In ATMega microcontroller based sensor node, there is a provision for sleep and awake mode. Due to operating this sensor node in sleep and active mode, the CPU time is being saved to a greater extend. This, in turn improves the energy consumption of the node at one end. On the other hand, due to the application of huffman source coding scheme, the number of bits required for the packet transmission as well as reception are reduced.

5. Conclusions

In this study, a secure lightweight algorithm based on Vernam cipher based cryptographic technique with Huffman source coding scheme is implemented on several processor based sensor nodes. From the result analysis, it is inferred that the proposed scheme is faster in performing computational task when compared to other existing schemes. This system model has comparable cycle count performance in computation and 12% less cycle count with respect to other schemes. In addition, the proposed scheme also consumes less energy consumption due to the application of source coding and sleep/awake mode operational facility of the processor based sensor node. With this, the 38% energy consumption was achieved in node level and in turn enhances the lifetime of the sensor network.

Table 1. Number of execution cycle count for different algorithmic implementations.

Algorithm	ARM7TDM microcontroller based sensor node	MSP 430 microcontroller based sensor node	ATMega 128 microcontroller based sensor node
RSA+SHA-1	536	468	434
ECC+SHA-1	432	374	356
Vernam cipher encryption (proposed scheme)	326	266	239

Table 2. Active mode Energy consumption of ATMega 128 microcontroller based sensor node after applying source coding.

Actual payload (bytes)	Energy consumed [E_1(μJ)]	Compressed Payload (bytes)	Energy consumed [E_2(μJ)]	Energy saved [$E_1 - E_2$(μJ)]
4	537.3	1	248.5	288.8
8	665.8	2	278.3	387.5
16	947.4	4	544.7	402.7
24	1078.7	6	597.8	480.9
32	1233.3	8	603.6	629.7

Although the level of security offered by the proposed scheme is limited due to energy constraints, in future, the security level offered by the scheme can be further enhanced using hybrid model security scheme. This, in turn, consumes more energy for performing computational task at node level. However, ultra low power optimized FPGAs are able to enhance the computational speed and power consumption in comparison to microcontrollers of commercial sensor nodes. The architecture based on the combination of microcontroller and FPGA can play a key role in the future wireless sensor node designs in fields where requires strong cryptography and data compression.

References

[1] Mohamed, E., Elminir, H., Riad, A. and Yuan, X.H. (2015) A Secure Data Routing Schema for WSN Using ECC and Momomorphic Encryption. *Journal of King Saud University—Computer and Information Sciences*, In Press, Corrected Proof—Note to users. http://dx.doi.org/10.1016/j.jksuci.2015.11.001

[2] Omar Rafik, M.B., Sidi, M.S. and Mohamed, F. (2015) A Novel Secure Aggregation Scheme for Wireless Sensor Networks Using Stateful Public Key Cryptography. *Ad Hoc Networks*, **32**, 98-113. http://dx.doi.org/10.1016/j.adhoc.2015.01.002

[3] Roy, S., Conti, M., Setia, S. and Jajodia, S. (2013) Secure Data Aggregation in Wireless Sensor Networks. *IEEE Transactions on Information Forensics and Security*, **7**, 1042-1052.

[4] Prakash, G L., Manjula, S.H., Venugopal and Patnaik, L.M. (2009) Secure Data Aggregation Using Clusters in Sensor Networks. *International Journal of Wireless Networks and Communications*, **1**, 93-101.

[5] Rout, R.R. and Ghosh, S.K. (2011) Enhancement of Lifetime Using Duty Cycle and Network Coding in Wireless Sensor Networks. *IEEE Transactions on Wireless Communications*, **12**, 656-667. http://dx.doi.org/10.1109/TWC.2012.111412.112124

[6] Zeng, Y.P., Cao, J.N., Zhang, S.G., Guo, S.Q. and Xie, L. (2010) Random Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks. *IEEE Journal on Communications*, **28**, 867-874. http://dx.doi.org/10.1109/jsac.2010.100606

[7] Selcuk Uluagac, A., Lee, C., Beyah, R. and Copeland, J. (2008) Designing Secure Protocols for Wireless Sensor Networks. *Springer*: *Wireless Algorithms Systems and Applications*, **11**, 503-514.

[8] Guo, Y., Hong, F., Guo, Z., Jin, Z. and Feng, Y. (2010) Event Oriented Data Aggregation in Sensor Networks. *IEEE* 28*th International Conference on Performance Computing and Communications*, Scottsdale, 14-16 December 2009, 25-32.

[9] Rasheed, A. and Mahapatra, R.N. (2012) The Three Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks. *IEEE Transactions on Parallel and Distributed Systems*, **23**, 958-965. http://dx.doi.org/10.1109/TPDS.2010.185

[10] Faye, S. and Myoupo, J.F. (2013) Secure and Energy Efficient Geocast Protocols for Wireless Sensor Networks Based on a Hierarchical Clustered Structure. *International Journal of Network Security*, **15**, 121-130.

[11] Xu, W.Y., Trappe, W. and Zhang, Y.Y. (2006) Jamming Sensor Networks: Attack and Defense Strategies. *IEEE Network*, **20**, 41-47. http://dx.doi.org/10.1109/MNET.2006.1637931

[12] Sen, J. (2009) A Survey on Wireless Sensor Network Security. *International Journal of Communication Networks and Information Security*, **1**, 59-82.

[13] Chaudhari, H.C. and Kadam, L.U. (2011) Wireless Sensor Networks: Security, Attacks and Challenges. *International Journal of Networking*, **1**, 4-16.

[14] Brooks, R., Govindaraju, P.Y., Vijaykrishnan, N. and Kandemir, M.T. (2007) Detection of Clones in Sensor Networks Using Random key Predistribution. *IEEE Transactions on Systems*, *Man*, *and Cybernetics*, *Part C* (*Applications and Reviews*), **37**, 1246-1258. http://dx.doi.org/10.1109/TSMCC.2007.905824

[15] Chan, H., Perrig, A. and Song, D. (2003) Random Key Pre distribution Schemes for Sensor Networks. *Proceedings of IEEE Symposium on Security and Privacy*, Washington, p. 197.