Challenges in Securing Wireless Sensor Networks

Heshem A. El Zouka
Department of Computer Engineering, College of Engineering and Technology
Arab Academy for Science & Technology and Maritime Transport,
Alexandria, Egypt
helzouka@aast.edu

Abstract — **Wireless sensor networks are highly prone to faults and errors due to their restrictive capabilities and limited resources. In this paper, some of the challenges facing the wireless sensor networks such as security, routing, computing capability, and battery power, will be discussed. We will focus on both security and authentication protocols in attempting to provide a security solution against known malicious attacks. Furthermore, utilizing the existing security protocols in wireless sensor networks has led us to propose a framework that incorporates authentication and encryption techniques in accordance with mobile agent technology in a way that reduces the energy consumption in such low power wireless sensor networks.**

Keywords-Security; Authentication; Routing; Energy efficient; Energy conserving; Agent-based architecture.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have recently attracted great attention due to their wide use in modern applications, such as military radio applications, environmental monitoring, and heath care industry. WSNs may consist of a large number of tiny and inexpensive sensor nodes that are densely deployed where the neighboring nodes may be very close to each other in a large area, collecting salient information from the target field. In a WSN, the base (sink) node is carefully positioned, so that it can communicate with all network nodes using the proper methods and protocols [1].

In general, the sensor nodes share a common predefined purpose to sense a predefined surrounding area being monitored and the sensed data is aggregated and transmitted to the base station where analysis can be performed to obtain some summary measures of the information provided by the sensor nodes. Thus, security became a necessity since sensor nodes are being small and less capable to provide tamper-resistant and their deployment is left unattended once dispersed over unprotected areas.

It is, therefore, difficult to determine whether the node participating in the routing domain is Byzantine [2] or indeed an authenticated node. The security risks and power consumption remain high-priority issues in designing WSNs [3]. Despite of these two issues, WSN has many features including flexible deployment, self-organizing, high reliability, and low-cost.

In section two, we are going to present the trends and challenges facing the development of new security models in WSNs. The third section presents the proposed security models with their respective advantages and disadvantages in details. The fourth section gathers everything together; our implementation is discussed along with all the simulation results obtained and a comparison of the results is presented. Section six draws a conclusion and future works.

II. LITERATURE SURVEY

WSN and Ad hoc networks [4] are getting more and more popular now. In fact, WSNs are inherited from ad hoc networks in the sense of being wide spread over geographical locations.

Ad hoc networks have no predefined, fixed infrastructure; they have no centralized controller or a fixed router [5]. Unlike wired and Mobile Ad hoc Networks, WSNs are infrastructure-less and can work in any environment as compared to the traditional computer networks.

The main difference between ad hoc networks and WSNs is that a WSN has reduced capabilities of the sensing nodes, such as reduced energy, computational power, no mobility, and limited transmission range [6]. The main components of sensor nodes are shown in Figure 1.

A. Energy Conservation

The limitations and the specific architecture of sensor nodes call for energy efficiency and secure authentication protocols. The feasibility of these inexpensive sensor networks is driven by the advances in Micro Electromechanical Systems (MEMS) technology [7], combined with low power, low cost CMOS logic. Through sensor networks, we are able to analyze data more accurately, gain more knowledge and improve our awareness of risk management issues.

Hence, it is quite essential to secure such data and employ strong authentication models while maintaining a reasonable level of energy dissipation.

 ISBN: 978-1-61208-296-7

In order to guarantee proper operation, sensor nodes must be supported by a power unit, which is usually in the form of a battery, however, in some cases, energy can be regenerated using solar cells. Energy from power scavenging techniques may only be stored in secondary (rechargeable) batteries and this can be a powerful combination in wireless sensor node environments where standard maintenance procedures like battery changing are impractical. Furthermore, when energy saving technique such as Dynamic Voltage Scaling (DVS) is used, it preserves energy and power.

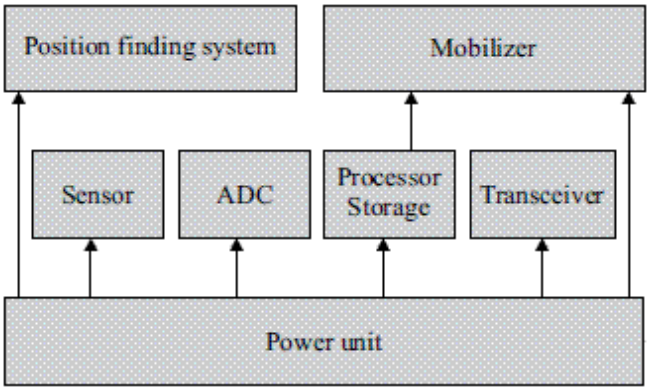

Figure 1. Sensor node components

During normal operation, every node periodically wakes up from sleep mode to communicate with its neighbors, and then goes to sleep again until the beginning of the next frame. In addition, due to the limited energy supply of the sensor nodes, it is assumed to be limited to use Public Key Cryptography (PKC) [8] in WSNs.

Recent research shows that PKC consumes a significant amount of computing resources and power. On the other hand, many studies have proved the falsehood of such assumptions and the ability to form a more secure communication under certain arrangements [9].

Meanwhile, new messages are temporarily queued to allow in-transit messages from node to node. Sensor nodes communicate with each other using a Request To Send / Clear to Send (RTS/CTS), and Acknowledgement (ACK) scheme, which provides both collision avoidance and reliable transmission scheme [10].

B. P2P Vulnerabilities

A Peer-to-Peer (P2P) network is a special type of network that has many characteristics over client-server manner. All wireless nodes are considered clients and servers and communicate directly with each other without an intermediate centralized hub. They all provide and consume network services. Peers are also routers as data passes through them to reach the destination node.

The difference between P2P networks and Cluster-based networks is illustrated in Figure 2 (a) and (b). P2P in WSNs has emerged to realize a computing architecture with no single-point of failure [11].

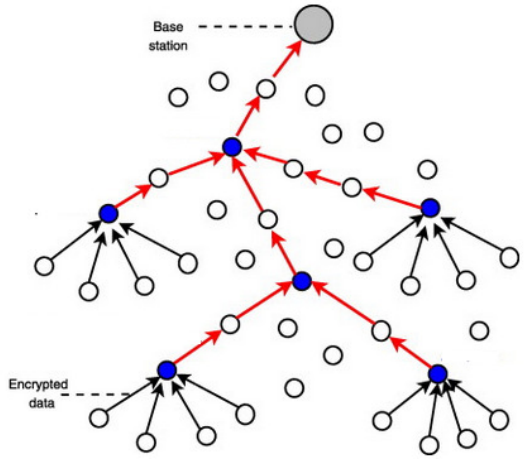

Figure 2. (a): Peer-to-Peer Communications in WSN

Its inherent scalability and lack of administration has made its cost virtually low. However, these features introduced a new set of vulnerabilities, such as false data injections and false data filtering, which have become an important issue for all WSNs. As opposed to the client-server networks, P2P has no always-on infrastructure servers [12].

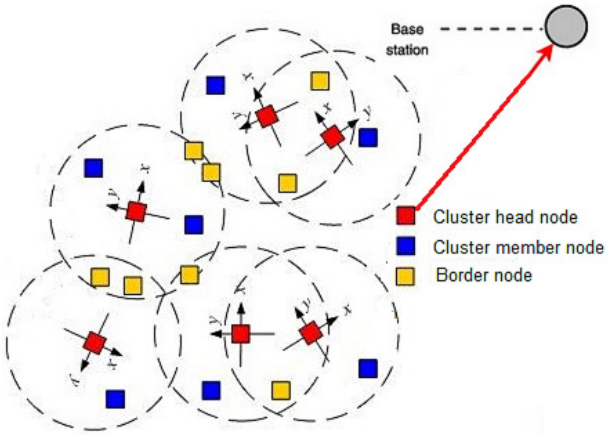

Figure 2. (b): Cluster Based Communications in WSN

The decentralized data source architecture eliminates the single-point of failure. This allows nodes to enter and leave the network frequently. Hence, a P2P network acts as a dynamic architecture. Moreover, decentralized networks have security issues since each node is responsible for controlling their data and resources. Hence, unauthenticated node within the cluster may send data that turns out to be a virus. This paper presents a combination of P2P and WSN networks to ease the development of models that rely on WSN functionality. As a result, we propose a network of, say, sensors, or P2P nodes, which allow integrating widely, distributed sensor nodes and other computing devices.

 ISBN: 978-1-61208-296-7

III. SECURITY IMPLICATIONS AND SOLUTIONS

In this paper, we performed some initial tests on the effectiveness of the envelope model that aims at securing the communication using Asymmetric Public key model, such as RSA algorithm, among the upper hierarchy, and symmetric model cryptography using AES among nodes. In this model, the network is divided into clusters and all the nodes inside each cluster will act as Cluster Heads (CHs) one with a different number of cycles in a fashion that maintain energy balancing. All nodes that are not CHs only communicate with their CH node using AES encryption model. On the other hand, all CHs are communicating with each other using strong encryption models, such as RSA cryptosystem, that make it essentially impossible for third party to decrypt. Therefore, the proposed security model guarantees data confidentiality as the keys cannot be detected due to the use of PKI cryptosystem. No malicious node can intercept or read the encrypted data of the sensed node. In later section of this paper, we will show how the performance of the sensor network is analyzed in terms of security, energy efficiency, and packet delivery rate.

We implemented our models based on the following assumptions: (1) the sensor nodes are deployed randomly with uniform distribution and (2) All nodes are homogeneneous and have the same initial energy. The energy model we have used is similar to [13], where E_{elec} = 50 nJ/bit as the dissipation of energy is used to run the transceiver circuit, and amplification of E_{elec} = 100 pJ/bit/m^2. The expansion of energy during transmission and reception of a k bit message is given by the following two equations; where, λ represents the path loss exponent and has a value ≥ 2.

$$E_{trans}(k, d) = E_{elec} * k + \in_{amp} * k * d^{\lambda} \quad (1)$$

$$E_{rec}(k) = E_{elec} * k \quad (2)$$

A. Envelope Routing Protocol

The routing attacks that affect the WSNs are also considered when implementing the envelope model. In case an attacker node changes any of the fields in a message or the destination of the message, such an attack is detected as the MAC algorithm performs the integrity check procedures. Another possible attack is sending malicious messages to nodes of the cluster. In this model, all nodes communication must go through the CH/BS, which keeps a list of all authenticated nodes. Therefore, the source of any message is checked against that list, which prohibits attackers from sending false data.

In our proposed model, we decided to employ the LEACH routing protocol. LEACH is currently one of the most famous communication protocols for WSNs [14]. LEACH is self-organizing and adaptive clustering protocol that is characterized by its feature of distribution the energy load among the sensing nodes within each cluster. Clusters, then, are created dynamically through a randomized rotation of cluster heads after each round. Data is aggregated by the CH and is sent to the BS after each round. LEACH assumes that the BS is fixed and located far from the sensors and all nodes in the network are homogeneous and energy constrained.

A cluster hierarchy will also aid us in utilizing an elected cluster head CH to perform asymmetric cryptosystem over the communication with other cluster heads, which decreases the communication overhead and bounds the asymmetric encryption operations to the elected cluster heads only. On the other hand, all nodes within the same cluster communicate using symmetric cryptosystem.

In case the attacker sends malicious data to cluster nodes, it will be detected since all the communicating nodes are trusted and authenticated by the base station itself as mentioned before. Hence, the source of any message is checked against that list, which prohibits attackers from sending malicious packets using forged or spoofed source addresses.

B. Envelope Authentication Protocol

In this section, we will show how the Mobile Agent (MA) is employed to enhance the authentication protocol of the sensing nodes. The design is similar to [15] in that the authentication of sensor nodes is controlled by the mobile agents platform using public key infrastructure and digital signature. The intelligence of a MA can be used to make dynamic decisions such as optimizing the travel plan, finding the next destination, and detecting link failures [16]. One of the major challenges of the deployment of MAs in WSNs includes secure transmission of agent as well as preventing unauthorized access to resources between communicating sensor nodes. However, MAs that move around the wireless networks are not safe because the remote hosts that accommodate the agents initiate all kinds of attacks.

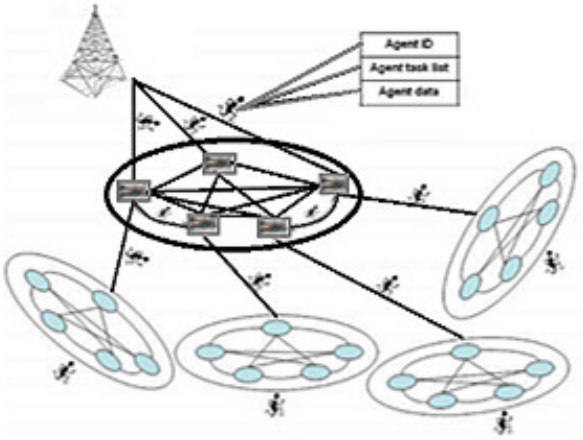

Figure 3. Middleware Mobile Agent Based Architecture

 ISBN: 978-1-61208-296-7

In addition, dispatching a set of low-level software modules to the sensor nodes is not an easy task, since it needs to interact with the sensor hardware devices within the network. Thus, to simulate this architecture, it is assumed that the modules are hard-coded into the memory of each node. Although some architecture allow the software developers to employ a node level OS, the developer still has to perform a single executable image to be configured manually into each node [17]. Overall, there is a strong need for developing a middleware environment that supports dynamic programming and simplify the complicated authentication / routing protocols in the sensor networks. Challenges in the development of Middleware approaches for WSNs constitute an emerging topic that is being investigated by a number of researchers [18].

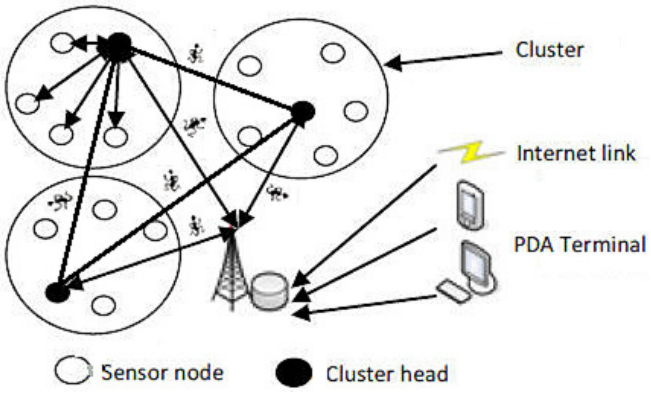

Figure 4. Envelope MA Based Architecture

Many of these approaches are based on mobile code (byte code) that runs on top of TinyOS [19], where a lightweight operating system specifically designed for such low power WSNs.

Application programs are broken up into small instruction segments, each of a single byte long, making it easier to be replicated and propagate through the network. Sending short instruction segments allows rapid deployment of aggregated message authentication code, as shown in Figure 3. Propagation of code segment is done whether by comparing code versions between neighbors (whenever possible) to update the routing information or by pursuing dynamic programming of sensor nodes. However, node's ability to allow code motion is highly limited.

To overcome this problem, our implementation utilizes how MA is used to perform the authentication mechanism without risking the security of the agents. As shown in Figure 4, the suggested architecture has been offered in two layers that aim to secure the execution results of MAs. The first layer aims to preserve the authenticity of the node via a combinational distributed and centralized agent server among the CHs hierarchies.

On the other hand, the second layer utilizes the authenticity of the agents on all nodes of the cluster. In this way, multiple MAs could be created and dispatched to the sensor nodes as soon as they are requested. For example, the central station could dispatch mobile software agents to perform authentication test and check communication between the sensor nodes. This will lead to minimize the communication overhead by eliminating unnecessary communications.

Data analysis and fault diagnosis MA algorithms can migrate over the network to perform collaborative monitoring and computational tasks. As shown in Figure 4, there is a centralized agent server per each cluster of the network, which maintains the security of the traversing agents within cluster.

That makes it essentially impossible for third party to attack the agents. In addition, the model guarantees data confidentiality as the keys cannot be detected due to the applied PKI in the clustering protocol, as discussed in the previous section of this paper.

C. Applied Compression and Hashing Algorithms

Due to energy limitation, a WSN faces to the challenge of lifetime. In order to minimize the energy consumed in the data communication, we need to decrease the time elapsed in data transmission.

In this section, we will investigate whether it is possible to save energy and load balancing in the WSNs by applying a compression technique over the data before sending. Thus, minimizing the size of the data, so that the radio transmission time will be reduced and the message will be less likely to be lost [20]. Compressing data helped us in saving energy as the data size to be communicated is smaller. Since accessing memory is quite expensive in energy, we searched for a compression algorithm that provides less memory access during execution time.

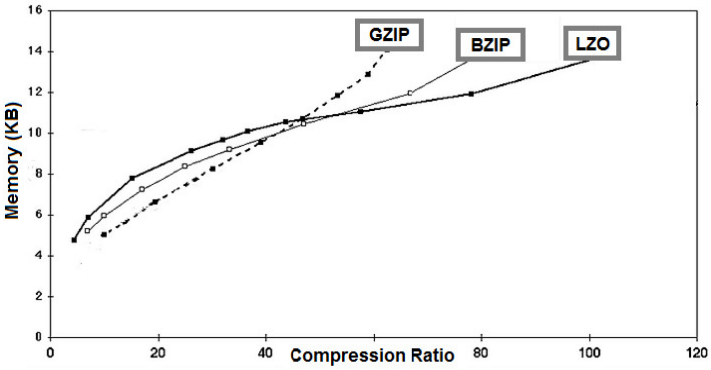

Figure 5. Speed and Compression Ratio Comparison

Figure 7 shows a comparison between different data compression algorithms, in terms of compression ratio and percentage root mean square difference.

Gzip is short for GNU zip [21]. It was created by Jean-Loup Gailly and Mark Adler. It is based on the Deflate algorithm and it usually used to find duplicate strings in the input data. The second occurrence of compression, a string

is replaced by a pointer that points to the previous string in the form of distance and length pair. Literals or match lengths are compressed with one Huffman tree [22], and match distances are compressed with another tree.

The trees are stored in a compact form at the start of each block. Duplicate strings are found using a hash table. All input strings of length 3 are inserted in the hash table. A hash index is computed for the next 3 bytes. If the hash chain for this index is not empty, all strings in the model will be compared with the current input string, and the longest match is selected. In this model, gzip for data compression was used as it offers fast compression technique, and executes fewer instructions per bit.

IV. COMPARATIVE PERFORMANCE ANALYSIS

Traditionally, the three main techniques for analyzing the performance of wired or wireless networks are analytical methods, computer simulation, and physical measurement. However, because of many constraints imposed on sensor networks, such as energy limitation, algorithms for sensor networks tend to be quite complex and usually defy analytical methods that have been proved to be fairly effective for traditional networks.

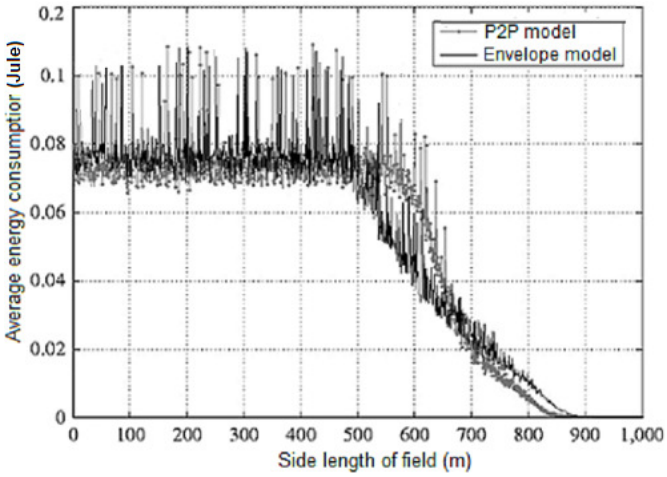

Figure 6. Total Energy Consumption

Furthermore, few sensor networks have come into existence, for there are still many unsolved research problems, so measurement is almost impossible. It appears that simulation is the only feasible approach to the quantitative analysis of sensor networks. In order to compare the implemented routing approaches; a powerful simulator was needed to measure the energy dissipation, end-to-end delay and throughput of both protocols.

The mixed mode in NS-2 using OTcl language [23] with underlying C++ classes made it complex to be used in our protocols. OMNET provided a simpler yet robust options, it enabled us to build the communication layers of the sensor nodes in an ease approach [24].

Figure 6 shows the energy consumption of a network when simulating the proposed envelope encryption model.

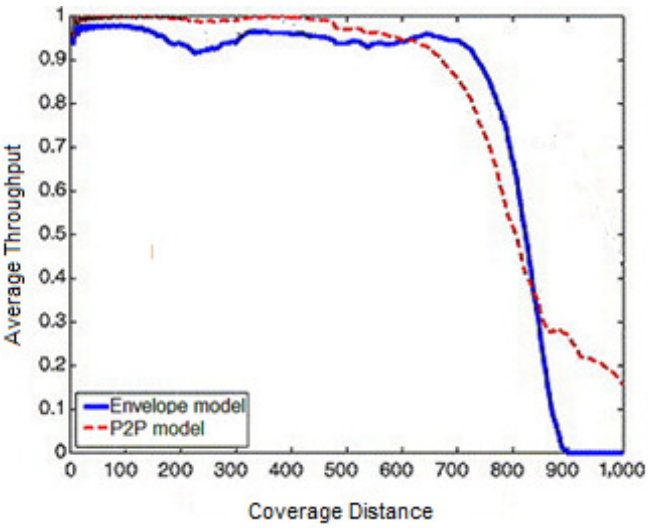

Figure 7. Average Throughput as a Function of the Field Size

The energy of the envelope model is the sum of energy of all nodes including the energy of the elected cluster heads. The consumed energy is shown to be lower for the envelope model as compared to the other models which use a public key cryptographic algorithm. In addition, the analysis provides a clear view of the percentage of nodes, which have considerable amount of energy compared to cluster head nodes of the nearly consumed ones. In the envelope model, the energy is more distributed over all the nodes, and more than 70% of the nodes in the envelope model preserved their energy as the energy is consumed mostly around the CHs. On the other hand, the model shows a more balanced energy consumption model, since all the nodes perform their own data transmission.

The radio of each non cluster head node is turned off till the node allocated time is reached, thus minimizing energy dissipation in these nodes. Once all data is received from all expected nodes in the cluster, the CH aggregates these data using the proposed MA mechanism and forwards them to the BS as one message in an effort to reduce the communication overhead. The storage requirement in the envelope model is also high, especially for CHs, since CHs store all the symmetric keys of the cluster nodes as well as any data to be sent or compressed. Each node in the node-to-node (n2n) connection model sends one message and as a result, asymmetric encryption is limited and this requires higher storage and computing complexity. Figure 7 illustrates the average throughput measured at the BS, the average throughput of the envelope model appears to be higher than the n2n connection model due to the aggregation of all data at the CHs. The envelope model provided a slight increase of 4% in the average throughput. The

 ISBN: 978-1-61208-296-7

analysis also showed that the average introduced delay in n2n approach is 27.4 sec while in the envelope model it reaches 34.5 sec due to the proposed security protocols.

V. CONCLUSION AND FUTURE WORK

In this paper, we surveyed the challenges and the proposed solutions and approaches for the security and routing protocols of WSNs. We then proposed a framework that secures the communications between the wireless nodes. In the first experiment, we implemented an envelope model that uses RSA asymmetric algorithm along with a symmetric algorithm in a hybrid manner to preserve the energy and increase the life time of WSN. In the second experiment, we examined how MA is employed to enhance the authentication protocol of the sensing nodes. To improve the performance of a middleware environment, the proposed envelope architecture is implemented using two security layers, one for establishing authenticity and one for generic trust that authenticates the distribution agents.

The analysis showed that the proposed envelope protocol provides a significant increase in the life of the entire network as more than 70% of the nodes reserved their energy while the consumption is limited to the CHs. Evaluating the effectiveness of employing a strong compression technique, the analysis showed that the GZIP experience fewer losses by sending fewer instructions per packet and the resulting compressed data size was roughly 2 times less than of original instruction data set size.

In the future, we plan to increase the scale of the network and to use more than one base station in our network, also we plan to make our protocols aware of data freshness by adding time stamp to the authenticated packet. We will explore more in dynamic compression techniques as well. Additionally, we plan to study the performance of our model on different motes and build a comparison over different architectures.

VI. REFERENCES

[1] A. Dearle, D. Balasubramaniam, J. Lewis, and R. Morrison, "A Component-Based Model and Language for Wireless Sensor Network Applications," 32nd Annual IEEE International on Computer Software and Applications, Turku, August 2008, pp. 1303-1308.

[2] P. Kiran Sree and I. Ramesh Babu, "Towards a Cellular Automata Based Network Intrusion Detection System with Power Level Metric in Wireless Adhoc Networks," Proceedings of 2008 International Conference on Advanced Computer Theory and Engineering, 2008, pp. 1071-1075.

[3] C. Chang, D. J. Nagel, and S. Muftic, "Assessment of Energy Consumption in Wireless Sensor Networks: A Case Study for Security Algorithms," In 4th IEEE International Conference on Mobile Ad Hoc and Sensor Systems (IEEE MASS 2007), Pisa, Italy, October 2007, pp. 1-6.

[4] T. El Maliki and J. M. Seigneur, "A security adaptation reference monitor (SARM) for highly dynamic wireless environments," in Proceedings of the 4th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE '10), July 2010 , pp. 63–68.

[5] C. Sreedhar, S. Vema, and P. Kasiviswanath, "A Survey on Security issues in Wireless ad hoc Routing Protocols, International Journal 2(2), 2010, pp. 224-232.

[6] L. Badia, M. Conti, S,K. Das, L. Lenzini, and H. Skalli, "Routing, interface assignment and related cross-layer issues in multiradio wireless mesh networks," In Guide to wireless Mesh Networks, Springer, London, 2009, pp. 147-170.

[7] MicroEelectroMechanical Systems (MEMS): http://mems.sandia.gov/. [Retrieved on June, 2013].

[8] W. Diffie and M. E. Hellman, "Multiuser cryptographic techniques," In Proceedings of National Computer Conference, New York City, AFIPS, June 1976 , pp. 109-112.

[9] S. Othman, A. Trad, and H youssef, "Performance Evaluation of Encryption Algorithm for Wireless Sensor Networks," International Conference on Information Technology and e-Service (ICITeS), March 2012, pp. 23-35.

[10] A. Pandey and R. Tripathi, "A Survey on Wireless Sensor Networks Security," International Journal of Computer Applications, vol. 3, no. 2, June 2010, pp. 8887 - 8975 .

[11] J. Sen, A Trust Based Detection Algorithm of Selfish Packet Dropping Nodes in Peer to Peer Wireless Mesh Network, In Recent Trends in Network Security and Applications, Springer, New York, 2010, pp. 528-537.

[12] T. Kavitha and D. Sridharan, "Security Vulnerabilities in Wireless Sensor Network: A Survey," Journal of Information Assurance and Security, vol. 5, no. 1, July 2010, pp. 31-44.

[13] S. Mostafa, H. El Zouka, and M. Abouelnasr, "Hybrid Encryption Secure Routing Protocols for Wireless Sensor Networks," Proceeding of the ISCA, First International Conference on Sensor Networks and Applications (SNA), San Francisco, November 2009, pp. 109-114

[14] S. Kumar, M. Singh, and D. Singh, "Routing Protocols in Wireless Sensor Networks - A Survey," International Journal of Computer Science & Engineering Survey (IJCSES), vol. 1, no. 2, November 2010, pp. 570-580.

[15] S. Srivastava and et al, "A Survey on Mobile Agent based Intrusion Detection System," IJCA Proceedings on International Symposium on Devices MEMS, Intelligent Systems & Communication (ISDMISC), New York, October 2011, pp. 19-24.

[16] M. Chen, T. Kwon, Y. Yuan, Y. Choi, and V. Leung, "Mobile Agent Based Directed Diffusion in Wireless Sensor Networks," Journal on Advances in Signal Processing, vol. 1, April 2007, pp. 219-242.

[17] G. Fortino, A. Garro, S. Mascillaro, and W. Russo, "Specifying WSN Applications through Agents Based on Events and States," International Conference on Sensor Technologies and Applications, Valencia, October 2007, pp. 463-468.

[18] F. Y. Xiong and L. Bai, "Interoperable Wireless Sensor Network Model Using Multi-Agent-Based Middleware," International Symposium on Intelligent Signal Processing and Communication Systems, Chengdu, December 2010, pp. 1-4.

[19] W. Munawar, M. Alizai, O. Landsiedel, and K. Wehrle, "Dynamic TinyOS: Modular and Transparent Incremental Code-Updates for Sensor Networks," In proceedings of the IEEE International Conference on Communications (ICC 2010), pp. 1-6.

[20] T. Arici, B. Gedik, Y. Altunbasak, and L. Liu, "PINCO: a Pipelined in-Network Compression Scheme for Data Collection in Wireless Sensor Networks," In Proceedings of 12th International Conference on Computer Communications and Networks (ICCCN)," October 2003, pp. 539-544.

[21] Gzip Home page. http//www.gzip.org [Retrieved on June, 2013].

[22] S. Mohajer, P. Pakzad, and A. Kakhbod, "Tight Bounds on the Redundancy of Huffman Codes," IEEE Information Theory Workshop (ITW), Punta del Este, Uruguay, March 2006, pp. 131-135

[23] The Network Simulator-NS-2. http://www.isi.edu/nsnam/ns [Retrieved on June, 2013].

[24] The OMNeT++ Simulator. http://www.omnetpp.org [Retrieved on June, 2013].

 ISBN: 978-1-61208-296-7