Advances in Electrical and Telecommunication Engineering (AETE)

AETE is a peer review journal of the Department of Electrical & Electronics Engineering, Ambrose Alli University, Nigeria

Two Layers Trust-Based Intrusion Prevention System for Wireless Sensor Networks

Oke, J. T., Agajo, J., Nuhu, B. K., Kolo, J. G. & Ajao, L. A.

Department of Computer Engineering, Federal University of Technology, Minna, Nigeria
agajojul@gmail.com

ARTICLE INFO

Article history:
Received 30 April 2018
Accepted 29 May 2018
Published 31 May 2018

Keywords:
Energy level
Intrusion detection system
Network performance
Trust value
Wireless sensor network

ABSTRACT

Security of a wireless sensor network is aimed at ensuring information confidentiality, authentication, integrity, availability and freshness is an important factor considering the criticality of the information being relayed. Hence, the need for an intrusion detection/prevention system. Conventional intrusion avoidance measures, such as encryption and authentication are not sufficient because they become useless in the event of a sensor node being compromised, hence, can only be seen as a first line of defence in the network after which intrusion detection schemes follow. In this paper, two layers trust-based intrusion detection system was developed for wireless sensor networks. A trust-based model is presented to detect intrusions to the network. Scenarios were created by using different set of weights. By injecting 2%, 5% and 10% malicious nodes from the 100 nodes considered, the results obtained were carefully observed. For scenario 2 (S2) with 2% and 5% malicious nodes injected, the model achieved the best result in all cases with an average detection accuracy of 97.8% while scenario 3 (S3) with 10% of malicious nodes introduced recorded the best performance with an average accuracy of 96%. Hence, the model will be suitable with combination of weights in S2 with small networks but when the scale of the network increases, the set of weights in S3 are best with the model.

1. Introduction

Wireless sensor network (WSN) can be referred to as a network of nodes (also known as motes) that work cooperatively to sample and control the parameters of the environment that surrounds them. Nodes in the network supportively route their data to a sink otherwise known as base station (BS) where the data can be logged and analysed (Matin & Islam, 2012). These nodes communicate wirelessly with one another and with the BS employing transceivers (Lagkas & Eleftherakis, 2014). WSN application is fast growing, as the distributed architecture among other attributes make them suitable for a variety of functions. However, wireless sensor nodes are constrained in terms of transmission range, memory, energy and computational power (Agajo *et* al., 2015; Rajeshkumar & Valluvan, 2016).

A major concern of researchers is whether the WSN can actually be secured, considering its fragile nature, as the network can be attacked to intercept messages/information (Iwendi & Allen, 2012). Passive attacks can be launched against the network privacy by unauthorised persons with the goal of monitoring and listening to the communication channel to extract meaningful information. The passive attacks include eavesdropping, traffic analysis and camouflage adversaries. When the packets contain control information, eavesdropping becomes very effective to the adversary than getting the information through the location

Please, cite this article as: Oke, J. T., Agajo, J., Nuhu, B. K., Kolo, J. G. & Ajao, L. A. (2018). Two Layers Trust-Based Intrusion Prevention System for Wireless Sensor Networks, *Advances in Electrical and Telecommunication Engineering, 1*(1), 23-29.

server (Padmavathi & Shanmugapriya, 2009). Eavesdropping attacks are either passive, when malicious nodes gather information by snooping on the message that is being transmitted through the wireless medium or active, when the malicious nodes gather information by sending requests to transmitters disguised as genuine nodes. In any case, the knowledge of the genuine nodes is important before a malicious node can disguise as it to query transmitters for information, hence, passive eavesdropping attack is necessary before an active eavesdropping attack can be successful (Dai *et al.*, 2015). Conversely, when an attacker monitors, listens to and modifies the data stream in the communication channel, the attack is termed an active attack. An active attack violates integrity and freshness of nodes data. Some of the active attacks on WSNs are Selective forwarding, jamming, hello flood, Sybil, sinkhole and wormhole attacks among others. Securing wireless sensor network has become necessary as this will ensure information confidentiality, authentication, and integrity (Matin & Islam, 2012).

Intrusion in the context of WSN is an unauthorized (unwanted) access to a sensor network by an attacker. The attacker either intrudes passively to gather information or eavesdrop or actively to forward harmful packet, drop packet or plant a hole node (Ismail *et al.*, 2014). Intrusion Detection Systems (IDSs) are developed and integrated into a network to detect any suspicious behaviour in the network using the nodes in the network. After detection provide alert to users and, possibly, reconfigure the network to take care of the malicious nodes.

Several intrusion detection systems exist (Garcia-Teodoro *et al.*, 2009; Gerrigagoitia *et al.*, 2009; Bao *et al.*, 2012; Kumar & Ramprasad, 2014) but most of them either provide low detection accuracy with too much false positives rate or incur a lot of overheads in computation, power and communication. IDS can be grouped into different classes depending on the considerations and purpose of grouping. Sobh (2006), classified IDS based on: intrusion type, intruder type, detection method, source of audit data, computing location of the collected data, infrastructure and usage frequency. According to Stetsko (2010), there are two major classes of IDS based on detection method: anomaly-based detection and signature-based detection. Sobh (2006) added a third class called specification-based detection. The three differ in the way they detect malicious nodes as can be seen in the subsequent sections. In this paper, a multi-layer trust-based intrusion prevention model was developed for wireless sensor networks.

2. Methodology

The wireless sensor network was divided into clusters, each cluster with a cluster head selected by the base station based on its energy level. The intrusion detection system (IDS) is hierarchical (two layers) in nature: cluster level and intermediate level. Figure 1 shows a single cluster in the network during simulation. It is a 500 by 300 meters deployment field. The simulation was carried out in a MATLAB environment.

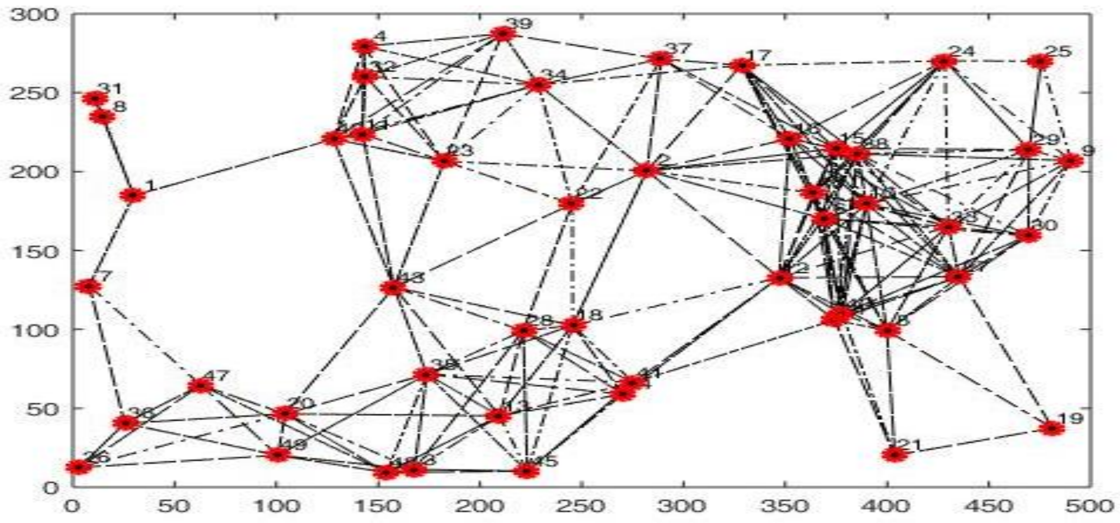

Figure 1: Cluster level network

2.1 Assumptions in the Network

The following are assumptions made in designing the network and IDS:

1. No intruder is expected at the initial deployment stage
2. All cluster heads are within the radio of at least one other cluster head
3. Aggregation occurred at each stage of the network.

2.2 Cluster Level Intrusion Detection (CLID)

In each cluster, the cluster head (CH) computes the trust level of all nodes under it at the end of each round. After the computation, if a node is found malicious, the CH isolates it from further network activities in the subsequent rounds. The following are the procedures:

1. CH computes the trust value of all sensor nodes in its cluster at the end of each round
2. If a node is found malicious, CH isolates the malicious node from further network activities
3. Nodes in the cluster stop forwarding or receiving packets from it in the subsequent rounds.

2.3 Network Level Intrusion Detection (NLID)

Similar to the CLID, the cluster heads (CHs) in the network relay data from their clusters to the base station. The base station computes the trust value of all CHs in the network at the end of every round. If found malicious, the base station excludes it from further network activities and assigns a new CH to the affected cluster.

2.4 Trust Value Computation Algorithm at Cluster and Intermediate Level

Based on the attributes of all the nodes/CHs shown in Table 1 and their residual energies, their trust values at the end of a round are computed using (1).

Table 1: Considered attributes of nodes

S/No	Attributes	Symbol
1	Packet Generating Rate	*NPg*
2	Packet Receiving rate	*NPR*
3	Packet Sending Rate	*NSR*

$$T_A = w_{e1} T_A^{NP} + w_{e2} T_A^{Energy} \quad (1)$$

where,

$$T_A^{NP} = \frac{1}{3}(w_1 A_1 + w_2 A_2 + w_3 A_3) \quad (2)$$

The first term of (1) is the trust component based on network performance of the node, which is further expanded (2); the second term is the component based on residual energy; W_{e1} and W_{e2} are weights assigned to the trust components, which add up to 1; w_1, w_2 and w_3 are weights manually assigned to attributes depending on their impacts on the trust and they add up to 1.

To confirm a node or CH as malicious, the CH or base station also computes the average trust value (T_{NA}) of all the neighbouring nodes or CHs of the concerned node/CH using (3) and an allowable threshold using (4).

$$AvgT_{NA} = \frac{1}{N}\sum_{i=1}^{N} T_{NA_i} \quad (3)$$

where, T_{NAi} are the trust values of the neighbours of the concerned node and N is the number of neighbours.

$$\text{Threshold} = /AvgT_{NA} - MinT_N/ \quad (4)$$

where: $MinT_N$ is the minimum trust value in the cluster or intermediate level as the case may be.

The process of detecting a malicious node using the above equations is shown in Figure 2. As can be seen in the figure, if the computed trust value of a node plus the threshold is less than the minimum threshold in the cluster (T_A + Threshold < MinimumT_N) or the computed threshold minus the threshold is greater than the maximum trust value in the cluster (T_A + Threshold > MaximumT_N), then the node is malicious. The process is the same at the intermediate level with the CHs replacing the nodes.

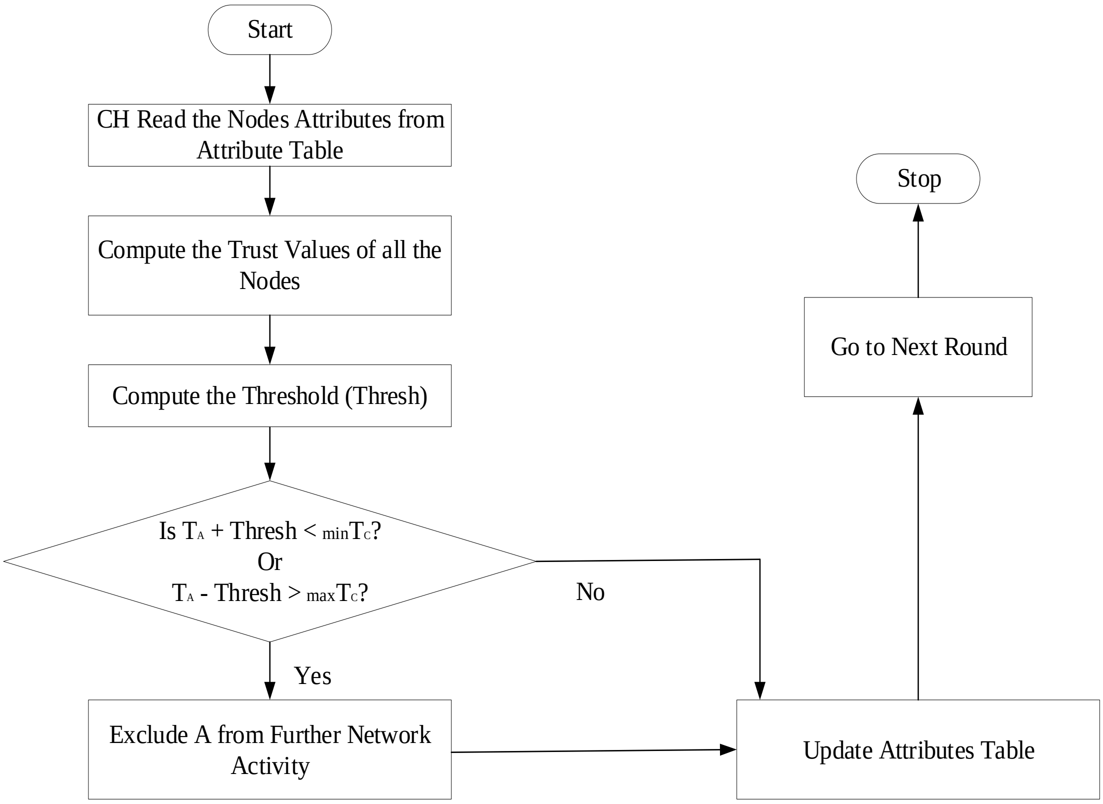
Start
CH Read the Nodes Attributes from Attribute Table
Compute the Trust Values of all the Nodes
Compute the Threshold (Thresh)
Is T_A + Thresh < $_{\min}T_C$?
Or
T_A - Thresh > $_{\max}T_C$?
No
Yes
Exclude A from Further Network Activity
Update Attributes Table
Go to Next Round
Stop

Figure 2: Flowchart for intrusion detection at cluster level

2.5 Performance Evaluation

The Nodes/CHs evaluation algorithm was evaluated when the malicious nodes in percentages of 2%, 5% and 10% were deliberately introduced into the network one after the other to see how they can be detected. Hence, the overall accuracy of the algorithms in detecting malicious nodes in the network was ascertained by (5) as follows:

$$Accuracy = \frac{T_P+T_N}{T_P+T_N+F_P+F_N} \tag{5}$$

Where T_p is the true positive, T_N is the true negative, F_N is the false negative and F_p is the false positive

3. Results and Discussion

The results obtained from the evaluation of the trust-based intrusion detection algorithm, is presented in Tables 2, 3 and 4 for different values of W_{e1}, W_{e2}, W_1, W_2 and W_3 as contained in (1) and (2) described in section 2.4. Careful observation from the Tables shows that, scenario 2 (S2), is the combination of weights that produced the best result using the model in all cases for fewer number of malicious nodes (< 10) recording an average accuracy of 97.8%. For malicious nodes of 10 and above, scenario 3 (S3) proved more effective with an average accuracy of 96%. The graph in Figure 3 shows number of malicious nodes returned, based on their Network performance and Residual Energy, $W_{\mathbf{e1}}$ **and** $W_{\mathbf{e2}}$ respectively, putting into account weight W_1, W_2 and W_3

Table 2: Results obtained after round two with $W_{e1} = W_{e2} = 0.5$

Parameters	Percentage of malicious nodes introduced														
	2%					5%					10%				
	S1	S2	S3	S4	S5	S1	S2	S3	S4	S5	S1	S2	S3	S4	S5
W_1	0.2	0.3	0.5	0.4	0.2	0.2	0.3	0.5	0.4	0.2	0.2	0.3	0.5	0.4	0.2
W_2	0.4	0.5	0.2	0.2	0.2	0.4	0.5	0.2	0.2	0.2	0.4	0.5	0.2	0.2	0.2
W_3	0.4	0.2	0.3	0.4	0.8	0.4	0.2	0.3	0.4	0.8	0.4	0.2	0.3	0.4	0.8
F_P	0	0	1	0	0	2	0	1	1	0	4	2	2	2	1
F_N	4	3	6	2	10	1	2	3	7	3	5	3	1	6	2
TP	2	2	1	2	2	3	5	4	4	5	6	8	8	8	9
T_N	94	95	92	96	88	94	93	92	88	92	85	87	89	84	88
Accuracy (%)	96	97	93	98	90	97	98	96	92	97	91	95	97	92	97

Table 3: Results obtained after round two with W_{e1} =0.6, W_{e2} = 0.4

Parameters	Percentage of malicious nodes introduced														
	2%					5%					10%				
	S1	S2	S3	S4	S5	S1	S2	S3	S4	S5	S1	S2	S3	S4	S5
W_1	0.2	0.3	0.5	0.4	0.2	0.2	0.3	0.5	0.4	0.2	0.2	0.3	0.5	0.4	0.2
W_2	0.4	0.5	0.2	0.2	0.2	0.4	0.5	0.2	0.2	0.2	0.4	0.5	0.2	0.2	0.2
W_3	0.4	0.2	0.3	0.4	0.8	0.4	0.2	0.3	0.4	0.8	0.4	0.2	0.3	0.4	0.8
F_P	1	0	0	1	1	1	1	0	1	1	0	3	2	4	2
F_N	5	2	3	1	2	5	2	3	1	2	6	4	1	3	2
TP	1	2	2	1	1	4	4	5	4	4	10	7	8	6	8
T_N	93	96	95	97	96	90	93	92	94	93	84	86	89	87	88
Accuracy (%)	94	98	97	98	97	94	97	97	98	97	94	93	97	93	96

Table 4: Results obtained after round two with W_{e1} =0.4, W_{e2} = 0.6

Parameters	Percentage of malicious nodes introduced														
	2%					5%					10%				
	S1	S2	S3	S4	S5	S1	S2	S3	S4	S5	S1	S2	S3	S4	S5
W_1	0.2	0.3	0.5	0.4	0.2	0.2	0.3	0.5	0.4	0.2	0.2	0.3	0.5	0.4	0.2
W_2	0.4	0.5	0.2	0.2	0.2	0.4	0.5	0.2	0.2	0.2	0.4	0.5	0.2	0.2	0.2
W_3	0.4	0.2	0.3	0.4	0.8	0.4	0.2	0.3	0.4	0.8	0.4	0.2	0.3	0.4	0.8
F_P	0	0	1	0	1	2	1	3	3	1	5	2	3	5	4
F_N	4	2	5	5	1	8	0	4	5	3	2	5	3	3	6
TP	2	2	1	2	1	3	4	2	2	4	5	8	7	5	6
T_N	94	96	93	93	97	87	95	91	90	92	88	85	87	87	84
Accuracy (%)	96	98	94	95	98	90	99	93	92	96	93	93	94	92	90

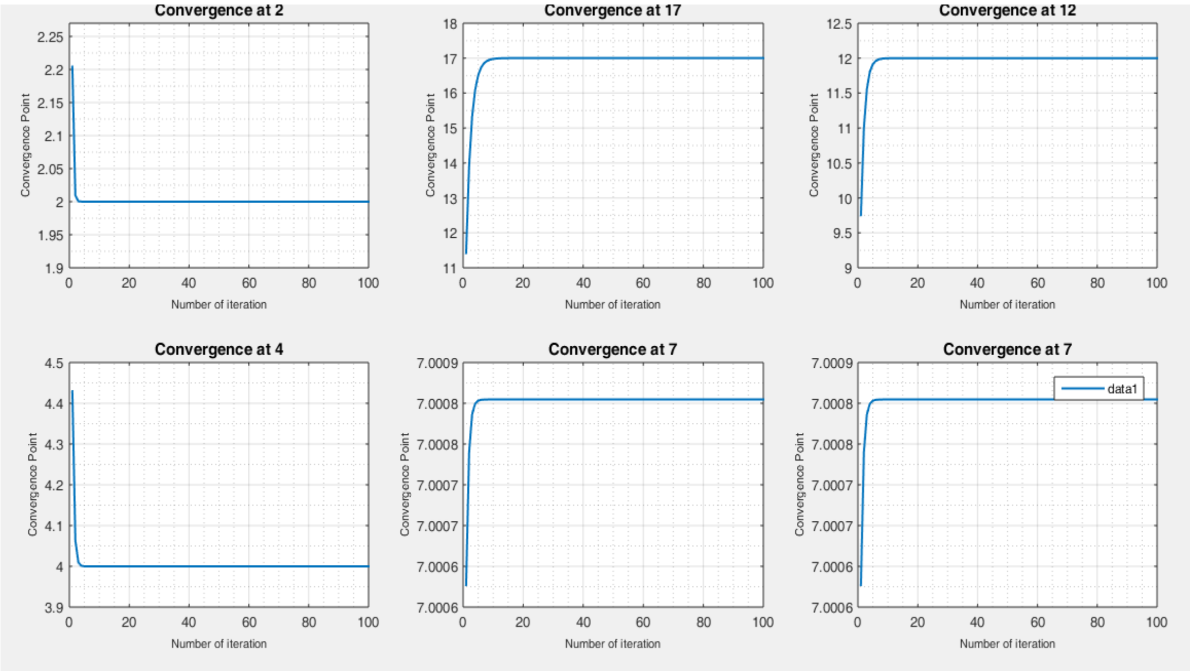

Figure 3: Convergence showing percentage of malicious nodes returned for the different scenarios

4. Conclusion

This work evolves security of a wireless sensor network to ensure information confidentiality, authentication, integrity, availability and freshness which are important factors in WSN, especially when we consider the criticality of the information relayed by such networks. To achieve that, there is need for an intrusion detection system to complement the conventional intrusion prevention measures, such as encryption and authentication. This work, implements a two layers trust-based intrusion detection model for wireless sensor networks through the development of a trust-based model that detects intrusions to the network. Different scenarios were created using different set of weights and malicious nodes were injecting in 2%, 5% and 10% from the 100 nodes considered in the simulation. From the several scenarios, an outstanding performance was recorded in scenario 2 (S2) with 2% and 5% malicious nodes injected, with an average detection accuracy of 97.8% while the best result with 10% of malicious nodes introduced was achieved in S3, with an average accuracy of 96%. Hence, the model will be suitable with combination of weights in S2 with small networks but when the scale of the network increases, the set of weights in S3 are best with the model.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

Agajo, J., Okhaifoh, J., Onyebuchi, N., Ekwueme E. U. (2015). Adaptive monitoring and localization of faulty node in a wireless sensor network, *American Scientific Research Journal for Engineering, Technology and Sciences*, 14(1): 77-93

Bao, F., Chen, I., Chang, M. & Cho, J., (2012). Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *IEEE Transactions on Network and Service Management*, 9(2): 169-183.

Dai, H., Wang, Q., Li, D., & Wong, R. C., (2015). On eavesdropping attacks in wireless sensor networks with directional antennas. *International Journal of Distributed Sensor Networks*, vol. 2015, 1-13

Garcia-Teodoro, P., Diaz-Verdejo, J., Macia-Fernandez, G. & Vazquez, E., (2009). Anomaly-based network intrusion detection: techniques, systems and challenges. *Journal of Computers and Security*, 28(1-2): 18-28.

Gerrigagoitia, K., Uribeetxeberria, R., Zurutuza, U., & Arenaza, I. (2012). Reputation-based intrusion detection system for wireless sensor networks. In *Complexity in Engineering (COMPENG)* IEEE*,* 1-5.

Ismail, B., Salvatore, D. M., & Ravi, S., (2014). A Survey of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 16(1): 266-282.

Iwendi, C. O. & Allen, A. R. (2012). Enhanced security technique for wireless sensor network nodes, *International Conference on Wireless Sensor Systems Conference*, Institute of Engineering Technology, IET United Kingdom

Kumar R. M. & Ramprasad A. V. (2014). Trust management based intrusion detection in wireless sensor networks. *International Journal of Innovative Research in Science, Engineering and Technology,* 3(3): 1025-1028

Lagkas, T. D., & Eleftherakis, G. (2014). An overview of wireless sensor networks: towards the realization of cooperative. *Handbook of Research on Progressive Trends in Wireless Communications and Networking*, 317.

Matin M. A. & Islam M. M. (2012), Overview of wireless sensor network, downloaded on 20/02/2017, from: http://cdn.intechopen.com/pdfs/38793/InTechOverview_of_wireless_sensor_network.pdf

Padmavathi, G. & Shanmugapriya, D., (2009). A Survey of attacks, security mechanisms and challenges in wireless sensor networks, *International Journal of Computer Science and Information Security*, *4*(1-2): 1-9

Rajeshkumar G. & Valluvan K. R., (2016). An energy aware trust based intrusion detection system with adaptive acknowledgement for wireless sensor network. *Wireless Peers Communication*. Springer

Sobh, T. S., (2006). Wired and wireless intrusion detection system: classifications, good characteristics and state-of-the-art. *Elsevier Journal of. Computer Standards and Interfaces*, 28(6): 670-694.

Stetsko, A. (2010). Intrusion detection for wireless sensor networks. Masaryk University, Faculty of Informatics, Brno, Czech Republic. http://is.muni.cz/th/184905/fi_r/thesis_topic.pdf