ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

An Efficient Behavior Trust EvaluationSystem for Wireless Sensor Networks

D. Ramya
Ratnavel Subramaniam College of Engineering and Technology,Dindigul, India
ramyait35@gmail.com

Abstract

Conventional trust management techniques developed for wired and wireless sensor networks are not well suited for applications due to their higher memory and power consumption. To overcome this an efficient Weighted Trust EvaluationSystem for Wireless Sensor Networks (WTES-WSN), is proposed in this paper. A trust detection system is proposed based on node identities and an enhanced trust evaluating approach is defined in cooperation between cluster heads.This approach significantly increases the system efficiency and reduces the cost of trust evaluation. Moreover a novel scheme based on behavior-trust evaluation and the hash table checker is used to detect malicious nodes is proposed in this paper. Also, theoretical and simulation results show that this scheme provides less memory, energy, and communication overheads as compared to the current trust management schemes. Furthermore, this approach enables us to detect and prevent malicious, selfish, and faulty nodes.

Keywords: Wireless sensor network, trust management, security, reputation.

Introduction

THE Wireless Sensor Network provides a new prototype for sensing and disseminating information from various environments, with the potential to serve many and diverse applications.WSN consists of a huge number of small sensor nodes that are grouped with analyzing, processing and communicating components and base station. The WSN authority can send queries to the base station and spread those queries to network. Hence base station act as a gateway between the WSN and external world. The applications of the WSN include Earth monitoring, health care monitoring, industrial monitoring etc., This feature of sensor networks makes them more susceptible to various attacks. So Wireless Sensor Networks need more security to withstand in critical areas. Cryptography and authentication approach provides security to WSN. But these approaches do not provide sufficient security in autonomous network. So a trust based methods are used for providing security to the network. For security enhancement and successful collaboration of sensor networks, trust based approach is essential.

Trust management ensures that every communicating nodes are trustworthy during authorization, authentication.This makes the security services more reliable and robust. Moreover, it will improve the system performance by increasing the cooperation among nodes. To evaluate the trustworthiness of the neighbors, a node not only monitors their explicit observations but also communicate with other nodes to exchange their opinions. The methods for attaining trust information and defining each node's trustworthiness are referred to as trust models. A trust model is mostly used for higher layer decisions such as routing and data aggregation, cluster head election and key distribution. Eventhough there are lots of designs in trusty models, their implementation has attracted nearly no attention. In Clusterwireless sensor networks (LEACH, EEHC, EC), clustering algorithms can efficiently improve the network scalability and throughput.

In clustering algorithms, each node isbound in clusters, and within each cluster, a node with strong computing power is selected as cluster head(CH). The clustering algorithm constructs a multilevel WSN structure, after several recursive iterations. This structure enables the restriction of bandwidth-consuming network operations such as flooding only to the intended clusters. A trust system in multihop clustering helps in the selection of trusted routing nodes through which a Sensor Node (SN) can send data to the CH. During intercluster communication, trust system also helps in the selection of trusted routing gateway nodes or other trusted CHs through which the sender node will forward data to the base station(BS).To yield the

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

global reputation for the node that can be used to evaluate the global trust degree of the node trust management system uses remote feedback. However, an open WSN consists of more malicious nodes. Feedback from these malicious nodes may yield wrong evaluation.Existing trust systems such as GTMS, HTMP, ATRM are failing to focus on the resource efficiency and dependability of the system.

To satisfy these requirements an efficient Weighted Trust Evaluation System for Wireless Sensor Networks (WTES-WSN) is designed in this paper. A weighted trust evaluation is used to detect the compromised nodes by monitoring its reported data. This paper focus on the dependable trust evaluating approach for cooperation between cluster heads.The indirect trust of a sensor node is calculated by cluster head. Thus each member in the cluster does not need to maintain the feedback from other members. This method will eliminate the possibility of a bad-mouthing attack by compromised sensor nodes.

The rest of the paper is organized as follows. Section II presents a description about the previous research which is relevant to the trust management system for wireless sensor networks. Section III involves the detailed description about the proposed method. Section IV presents the performance analysis. This paper concludes in Section V.

Related Work

This section analysis the previous work done for a trust system for clustered wireless sensor networks. *J. Alves, et al* described the operation of adaptive wireless sensor networks applications with real-time and dependability requirements. LQER routing protocol is considered to show how it must be changed to incorporate real-time requirements and solve them in an efficient way[1].Wireless sensor networks are exposed to many kinds of invasion as they have limited memory, battery life and limited power. Intrusion detection is a solution to WSN against various kinds of attacks. *E. Darra and S. K. Katsikas*reviewed the types of attacks against wireless sensor networks and relevant intrusion detection approach[2].\

*Y. Yu, et al*presented an extensive method to analyze the various types of attacks and countermeasures related to trust schemes in wireless sensor networks. An open field and further idea with trust mechanisms in WSN is discussed[3].In ES-MHRT the transmitter analyzes the status of delivery report from the receiver only. This will take more time to analyze the reliable route. Because of this transmitter couldn't forward the data in efficient manner, which affects the network performance parameters such as bandwidth and throughput. To overcome these problems *I. Rijin, et al*proposed an effective distributed monitoring system to improve the lifetime the wireless sensor network[4].

Toestimate the overall trust of a sensor node*F. Bao, et al* considered multidimensional trust attributes derived from communication and social networks. To efficiently deal with malicious nodes, a huge scalable cluster based hierarchical trust management protocol for wireless sensor network is presented. The proposed method is applied in geographic routing and trust based intrusion detection[5].*H. Alzaid, et al*proposed a comprehensive analysis for current reputation-based trust systems by evaluating the state of art. Previous reputation based trust systems were applied to identify abnormal activities and enhance the trustworthiness among sensors. But it did not investigate the robustness against reputation related attacks[6].

V. S. Dhulipala, et al proposed a Heuristic approach based trust worthy architecture for WSN. It concentrated on the collaborative mechanism for trust evaluation and maintenance. The proposed method was capable of satisfying reliability,mobility for better communication in different applications[7].*K. Shaila, et al* presented an anonymity cluster based trust management algorithm (ACTM). The proposed method increased the security level and provided a efficient way for communication[8]. *R. Feng, et al*proposed a security localization algorithm based on trust mechanism. It was used to analyze the mischievous beacon nodes in UnderWater Sensor Network (UWSN). This proposed method found the initial trust value by using the beta distribution and the required trust update weight was set. Trust Filter Mechanism (TFM) algorithm was developed to calculate the trust value and the cluster head node decide whether the beacon node is acceptable or not[9].

J. Lopez, et al list out the method for developing a best trust management system for WSN and analyzed the state of art related to those methods[10].Wireless sensor networks are hugely used in different environments to perform various events such as recovery, disaster management, target monitoring and a number of events in smart environments. In such tasks node localization is intrinsically one of the system parameters.*A. Pal* reviewed different methods of node localization in wireless sensor networks[11].Based on ant colony systems*F. G. Mármol and G. M. Pérez*proposed a bio-inspired trust and reputation model called

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

BTRM-WSN. This method is proposed for improving the level of security in a restrictive environment[12].*T. Kavitha and D. Sridharan*compared the security issues and the basic information about wired sensor network and wireless sensor network. Description of the typical attacks on sensor network and the security issues related to sensor networks are also discussed[13].

Trust MAnagement System Model

Network Architecture

Cluster based WSN consisting of multiple clusters, that each node in the clustered WSN model can be determined as a Cluster Head (CH) or Sensor Node (SN) or Forwarding Node (FN). Cluster Head directly interacted by their Sensor Node. Cluster Head can transmit the combined data to the central base station or the destination node (or sink node)through other Cluster Head. We assume that nodes are organized into clusters with the help of a proposed cluster scheme.A number of SNs are organized as a group and it is controlled by a CH. Hence, every sensor node communicates only with its CH. Let us consider the CHs and BSs are trustful and won't be compromised. Each CH provides two way communications. One with sensor node and another with base station. BS provide multihop routing packets from SNs and CHs within their range. Based on the information obtained from the SNs, CHs compute the aggregation result and informs the information to BSs. It is important for CHs to monitor whether the information collected from the SNs are correct or not. The network architecture is shown in Fig.1.

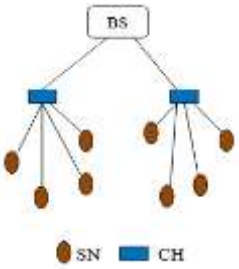

Fig.1.Network Architecture

WTES-WSNproposed two levels of trust detection: SN trust level and CH trust level. SN trust level has two kinds of relationship: SN-to-SN direct trust and CH-to-SN feedback trust. Likewise CH trust level has CH-to-CH direct trust and BS-to-CH feedback trust.Generally trust values can be a real number between 0 and 1 or an integer between 0 and 100. In this paper the trust value is assigned as an unsigned integer in the interval between 0 and 10, this only needs 4 bits of memory space. This will reduce the memory consumption. The architecture of the proposed method is shown in the Fig.2.

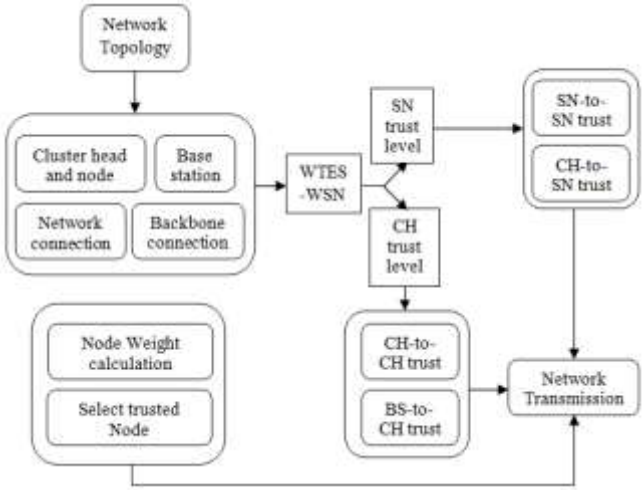

Fig.2.Proposed System Architecture

SN-to-SN direct trust : Sensor node calculates the trust value of its neighbors based on direct trust and feedback trust. Direct trust is calculated by the number of successful communication and unsuccessful communication. Let us consider node l transmits a message to cluster head $\mathcal{b}$ via node m. Node $a$checks whether the node m transmit the message to CH . If node a does not listen the retransmission of the packet within a threshold time from its neighboring node m, then a will be considered as communication failure. Trust estimation of SNs is defined as

$$S_{l,m}(\Delta t) = \left[\left(\frac{10 \times f_{l,m}(\Delta t)}{f_{l,m}(\Delta t)+g_{l,m}(\Delta t)}\right)\left(\frac{1}{\sqrt{g_{l,m}(\Delta t)}}\right)\right] \quad (1)$$

where Δt is a window of time. As time elapses, the window adds newer experience but forgets the previous old experience. $f_{l,m}(\Delta t)$ is the total number of successful interactions and $g_{l,m}(\Delta t) \neq 0$ is the total number of unsuccessful interactions of node l with m during time Δt. If $f_{l,m}(\Delta t) \neq 0$ and $g_{l,m}(\Delta t) = 0$, we set $S_{l,m}(\Delta t)$ =10. When there is no interactions between node l and m during time Δt, the sum of $f_{l,m}(\Delta t)$ *and* $g_{l,m}(\Delta t)$ is 0. $S_{l,m}(\Delta t)$ is used for calculating the SN-to-SN direct trust method.

*CH-to-SN feedback trust:*WTES-WSN does not utilize the a broadcast based strategy and instead sets the indirect trust value is based on the feedback reported by the CH about a specific node. Thus, each SN does not need to share trust information with its

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

neighbors. This mechanism has effective mitigation of the effect of malicious feedback, thereby reducing the networking risk in an open WSN environment. Given that the feedback between SNs need not be considered, this mechanism can significantly reduce network communication overhead, thus improving system resource efficiency.For example if a node a wants to communicate with node m, the transmitter node checks whether it has any previous communication with the destination node during a specific time interval. If the previous communication record exists, then a makes a decision directly. Otherwise node a will send a feedback request to its Cluster Head b.

$S_{l,m}(\Delta t)$ is also considered as $D_{n,m}(\Delta t)$. It is used for calculating the CH-to-SN indirect trust method. Consider that there are $(v-1)$ sensor nodes in a cluster. Within the cluster the CH ch will periodically transmit the request packet. Every SNs in the cluster will forward their trust values toward other SNs to ch . The equation of $D_{ch,m}(\Delta t)$ is defined as

$$D_{ch,m}(\Delta t) = \lceil 10 \times H(\beta(p|c,e)) \rceil \quad (2)$$

Where p denotes the posterior probabilities of binary events (c,e). e is the amount of negative feedback towards the node m. $H(\beta(p|c,e)$ is the probability expectation value of beta distribution $\beta(p|c,e)$. $H(\beta(p|c,e) = (c+1)/(c+e+2)$. With an increase in the number of unsuccessful interactions $1/\sqrt{g_{l,m}(\Delta t)}$ rapidly equals to 0. This feature effectively avoids sudden attacks from malicious nodes with higher accumulated trustworthiness.

CH-to-CH direct trust:The selection of CH is a very important for dependable communication. Because CH can forward the aggregated data to the central BS through CHs. In CH-to-CH communication, the direct trust value is calculated according to the number of successful and unsuccessful interactions. When a CH b wants to communicate with another CHq, it will send a feedback request to the BS. The BS periodically collects all CHs for their trust ratings on their neighbors. After receiving the results from the CHs, the BS will combine them to form an effective trust value. Thus this mechanism can greatly reduce the network communication overhead and improve the system efficiency. For example, if a CH $b$wants to interact with another CH q, b initially calculates CH-to-CH direct trust for x based on past communication records with q during specific time interval. Meanwhile b sends a feedback request to the BS. After receiving the request, the BS will send a response message to$b$, in which q's feedback trust value is combined. Then b will combine these trusted sources into a group trust detection, after b will make a final decision based on q's group trust value. The direct trust value between CH b toward another CH q is defined as:

$$C_{b,q}(\Delta t) = \left\lceil \left(\frac{10 \times F_{b,q}(\Delta t)}{F_{b,q}(\Delta t) + G_{b,q}(\Delta t)} \right) \left(\frac{1}{\sqrt{G_{b,q}(\Delta t)}} \right) \right\rceil \quad (3)$$

where $G_{b,q}(\Delta t) \neq 0$. $F_{b,q}(\Delta t)$and $G_{b,q}(\Delta t)$ are the total number of successful and unsuccessful interactions of CH b with CH q during time window Δt respectively. When $F_{b,q}(\Delta t) \neq 0$ and $G_{b,q}(\Delta t) = 0$, $C_{b,q}(\Delta t)$ is set as 10.

BS-to-CH feedback trust: Let us consider$z$ number of CHs exists in a network. Within the cluster, the base station bs will periodically broadcast the request packet. All CHs in the network will transmit their trust values toward other CHs to bs. Similar to the previous method, enhanced beta probability density function is used to determine for BS-to-CH feedback trust.

$$L_{bs,q}(\Delta t) = \left\lceil \frac{10 \times H\left(\beta(p|d,\sigma)\right) + \overline{C_{y,q}}(\Delta t)}{2} \right\rceil \quad (4)$$

Where p denotes the posterior probabilities of binary events (d,σ), d is the positive feedback and σ is the amount of negative feedback. The probability expectation value of beta distribution function $\beta(p|d,\sigma)$ is:

$$H\left(\beta(p|d,\sigma)\right) = \frac{d+1}{d+\sigma+2} \quad (5)$$

$\overline{C_{y,q}}$ is the average value of aggregates feedback from $(d+\sigma)$ CHs in the network:

$$\overline{C_{y,q}}\,(\Delta t) = \frac{\sum_{y=1}^{d+\sigma} C_{y,q}(\Delta t)}{d+\sigma} \quad (6)$$

Where $C_{y,q}(\Delta t)$ is the feedback of CH y toward CH q.This technique considers the quality of each feedback $C_{y,q}(\Delta t)$ with the amount of feedback $(d+\sigma)$.

Behavior Based Trust Evaluation Technology

To address the network security problem, a behavior based trust evaluation technology is proposed, which is used to check the malicious nodes in the cluster. Put the malware behavior in hash table.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

If any behavior of the cluster is match to the hash table assume that it is a malware , otherwise it is a trust cluster. Hash table has the dynamic updating feature that is used to update our malware detection methodology for future use. Hash table has the specific field to identify malware cluster. If the cluster is not detested as a malware, assume that the cluster is trust cluster, this has been update it to host environment. So there is no malware in the host environment. The behavior based trust evalution is shown in the Fig.3.

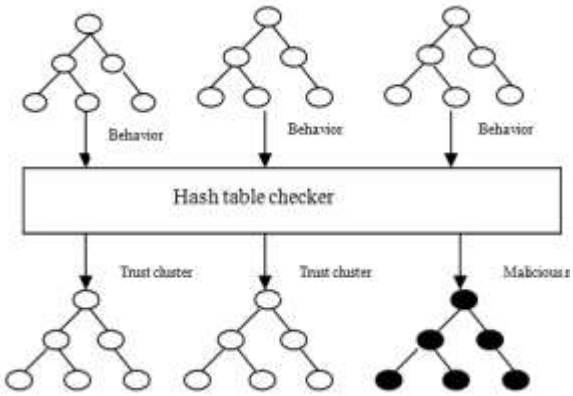

Fig.3. Behavior based trust evaluation

The algoritm is used to finding the behavior of the malware nodes.

Algorithm 1. Finding the type of a behavior
INPUT: behavior X
1: SN = HashFunc(X.object,HashTable1);
2: IF(HashTable1(SN).B = false)
3: RETURN no behavior;
4: END
5: IF(HashTable1(SN).C = false)
6: RETURN HashTable1(SN).T;
7: END
8: FOR each behavior Y in the OverTable
9: IF((Y.object = X.object) AND
(Y.parameter = X.parameter) AND
(Y.operation = X.operation))
10: RETURN Y.type;
11: END

Performance Analysis

This section presents the performance evaluation of the proposed WTES-WSN method. The performance is evaluated based on the following measures:

Communication overhead analysis

Fig.4. Shows the comparison of the various trust management system under large-scale clustered WSN. From the graph, the WTES-WSN requires minimum communication overhead than the GTMS and ATRM systems. The proposed system is highly suitable for large scale WSNs with either a small or large size of clusters.

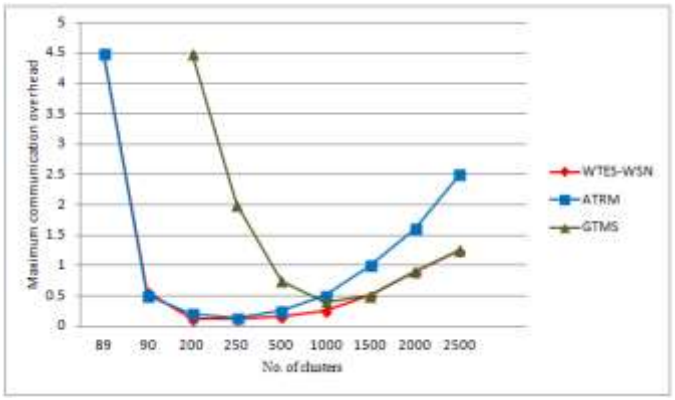

Fig.4. Communication overhead analysis

Storage overhead at SN level

Fig.5 shows the storage overhead of the trust management system under a clustered WSN environment. From the figure, the WTES - WSN system consumes less storage memory than the GTMS system at the SN level.

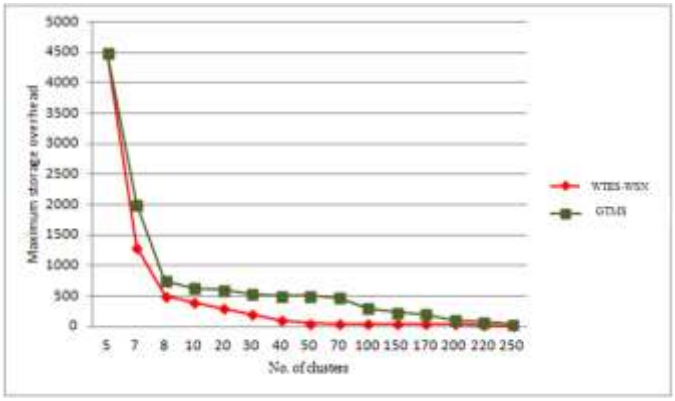

Fig.5. Storage overhead at SN level

Storage overhead at CH level

Fig.6 shows that as the number of clusters increases in the network, the WTES-WSN provides less storage overhead at the CH level. This indicates that WTES-WSN is more suitable for large scale WSNs having a small size of clusters.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

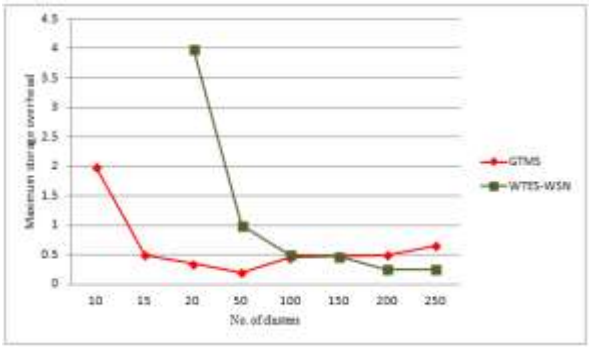

Fig.6. Storage overhead at CH level

Conclusion

The proposed WTES-WSN eliminates the feedback between nodes thus improves the overall system efficiency and reducing the effect of malicious nodes. The behavior trust evaluation method and cooperation between CHs for trust calculation detects and prevents the malicious and faulty CHs. Selfish and malicious nodes effectively and solve the security problems for node failure. Trust evaluation algorithm based on behavior strategy, which successfully underlines the, subjectively and usability of trust. The performance analysis shows that the proposed method consumes less memory and well suited for large scale clustered WSNs. If the control behavior of the trust and energy information can be accredited reasonably, the achievement of the routing in security and energy-efficient will reach optimal.As a future work, we target this controlling of optimal parameters.

References

[1] *Zhiyong shan, Xin wang, and Tzi-cker chiveh "Malware clearance for secure commitment of OS- Level Virtual Machines" in Dependable and secure computing, 2013.*

[2] *J. Alves, et al., "Middleware Support for Adaptive Real-Time Applications in Wireless Sensor Networks," in Dependable Computing, ed: Springer, 2013, pp. 16-23.*

[3] *E. Darra and S. K. Katsikas, "Attack detection capabilities of intrusion detection systems for Wireless Sensor Networks," in Information, Intelligence, Systems and Applications (IISA), 2013 Fourth International Conference on, 2013, pp. 1-7.*

[4] *Y. Yu, et al., "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," Journal of Network and Computer Applications, vol. 35, pp. 867-880, 2012.*

[5] *I. Rijin, et al., "Development of an Enhanced Efficient Secured Multi-Hop Routing Technique for Wireless Sensor Networks," Development, vol. 1, 2013.*

[6] *F. Bao, et al., "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," Network and Service Management, IEEE Transactions on, vol. 9, pp. 169-183, 2012.*

[7] *H. Alzaid, et al., "Reputation-Based Trust Systems for Wireless Sensor Networks: A Comprehensive Review," in Trust Management VII, ed: Springer, 2013, pp. 66-82.*

[8] *V. S. Dhulipala, et al., "A Novel Heuristic Approach Based Trust Worthy Architecture for Wireless Sensor Networks," Wireless Personal Communications, pp. 1-17, 2013*

[9] *K. Shaila, et al., "ACTM: Anonymity Cluster Based Trust Management in Wireless Sensor Networks," in Advances in Communication, Network, and Computing, ed: Springer, 2012, pp. 75-80.*

[10] *R. Feng, et al., "Trust Management Scheme Based on DS Evidence Theory for Wireless Sensor Networks," International Journal of Distributed Sensor Networks, vol. 2013, 2013.*

[11] *J. Lopez, et al., "Trust management systems for wireless sensor networks: Best practices," Computer Communications, vol. 33, pp. 1086-1093, 2010.*

[12] *A. Pal, "Localization algorithms in wireless sensor networks: Current approaches and future challenges," Network Protocols and Algorithms, vol. 2, pp. 45-73, 2010.*

[13] *F. G. Mármol and G. M. Pérez, "Providing trust in wireless sensor networks using a bio-inspired technique," Telecommunication Systems, vol. 46, pp. 163-180, 2011.*

[14] *T. Kavitha and D. Sridharan, "Security vulnerabilities in wireless sensor networks: A survey," Journal of information Assurance and Security, vol. 5, pp. 31-44, 2010.*