AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Implementation of Secure Fuzzy Based Authenticated Routing In Wireless Sensor Networks

[1]M.Balamurugan and [2]Dr.P.Manimegalai

[1]*Research Scholar, Karpagam University, Karpagam Academy of Higher Education, Coimbatore, India*
[2]*Professor, Department of ECE, Karpagam University, Karpagam Academy of Higher Education, Coimbatore, India.*

Address For Correspondence:
M.Balamurugan, Research Scholar, Karpagam University, Karpagam Academy of Higher Education, Coimbatore, India.
E-mail: sabaalu@gmail.com

ARTICLE INFO

Article history:
Received 11 September 2016
Accepted 10 November 2016
Published 28 November 2016

Keywords:
WSN, interruption finding Scheme, Fuzzy based Security system, Clock based Authentication, Data integrity, Certificate, Clock based determination, Malicious, Mobility, packet delivery ratio, Detection efficiency and packet latency.

ABSTRACT

Sensor node is an indivisible part of Wireless sensor network where it has no infrastructure. Background: In the past, interruption finding scheme is used to find the attacks in network effectively. Most of the systems are able to find attacks, which have maximum fake request. Objective: Proposed Fuzzy based Secure Intrusion Detection System (FSIDS) for detecting misbehavior of intruder and providing authentication as well as data integrity. To achieve this, grouping the nodes to perform routing is recognized that depends on hope of neighbor nodes in random topology. Certificate based trust recommendation is estimated based on packet identification, certification revocation record and packet receiving capability etc. Including this, clock based intrusion detection is also proposed for identifying and isolating the malicious nodes in network. Results: Security is also enhanced with the proposed IDS using fuzzy encryption and decryption to provide data integrity and authentication. Simulation results shows that the FSIDS provides better detection efficiency, packet delivery, minimum packet latency, efficient authentication and minimum overhead than compared to existing schemes.

INTRODUCTION

WSNs -Wireless Sensor Networks have collection of sensor nodes. Sensor nodes include the ability to it healing and controlling intruder nodes. It is decentralized and distributed in nature where communication carried on many intermediate nodes in network. Main goal of a sensor node is to gather information from its surrounding environment and broadcast data destination node. Sensor network contains various applications and are used in scenarios such as detecting node position updating, analyze network infrastructure and performance, and environment monitoring and military applications. Mostly sensor nodes are allowed in military environment, wired communication is blocked (Khan, S., *et al*., 2010; Khan, S., *et al*., 2014). WSNs have malicious nodes and unfriendly infrastructure that nodes are forever discovered to objective security problems. Furthermore, self-organizing character, minimum battery power deliver, carry restricted bandwidth, distributed operations using open wireless middle, many intermediate nodes in path cause traffic in packet transmission, and habit on remaining nodes have various features of sensor networks, that indicates so many protection issues at all layers of the OSI model.

Wireless sensor nodes are located with sleep and wake mode energy consumption is reduced. Network reality is improved and thus a need is arisen for the varied network consumption (Baiah, C., M. Poonam, 2014). The heterogeneous network operation has been mathematically improved by simulations in much network area and in some network operations model (Krasimira Kapitanova Sang H. Son, Kyoung-Don Kang, 2011). Some

ToCite ThisArticle:M. Balamurugan and Dr.P.Manimegalai.,Implementation Of Secure Fuzzy Based Authenticated Routing In Wireless Sensor Networks. ***Aust. J. Basic & Appl. Sci.,****10(16): 305-313, 2016*

fundamental knowledge in this hybrid deployment of the network is also surveyed to prolong lifetime of network. There is an extreme improvement in the network assistance and thus the position of these network servers damages the network's performance. (Hu, W., *et al*., 2010) Sensor nodes are more trustworthiness for collection information from network environment.

Malicious node detection in the wireless sensor networks is used in finding attacks. It is a mechanism in the networks to find the existence of unsuitable and inaccurate updating its location of attacker node that uses a more energy in the identification scheme (Nguyen, T., *et al*., 2010). Therefore identifying discarded attempts at the stages of processing and disabling in the network such as the internet is done by a design named IDS-Intrusion Detection System plan. This plays a input task in the network protection. Attack is nothing but the illegal login or contact to the system or network. Or it could be a group of process from some part of the network that would break the protection aspects of a resource (Gope, P., T. Hwang, 2015). There are many major techniques, specifically misuse identification and irregularity identification. In initial technique detects any illegal use of the signatures when the next technique detects the analysis of an incident. While these two techniques detect any violation, then they increase an alarm warning sign. That sign will caution the network (Srivastava, P.K., *et al*., 2012).

Outside user are normally involved in processing concurrent data from the sensor nodes (Chia-Fen Hsieh, *et al*., 2014; Chong Eik Loo, *et al*., 2006). This situation to allow external users to process the concurrent data straight from desired sensor nodes with not linking the intermediate nodes, this is a large concern that significant data is well secured from attacker node, misbehaving changes, illegal process. Therefore, the user verification constitutes a necessary protection technique for user to be genuine primary by the sensor nodes earlier than being decided the right to process information. (Gulshan Kumar and Krishan Kumar, 2014; Lee, J.J., *et al*., 2012). This structural design can be useful in various uses such as in a health-care environment, in that case, permanent monitoring of environmental status will be gathered by sensor nodes (Yang, D., *et al*., 2012; Gope, P., T. Hwang, 2016). Then a rightful server can obtain that information directly from the sensor nodes. Therefore, this technique can bring more benefits to both the server and user in several uses like a bio-Monitoring.

An IDS is also survey to as a next line of protection that used for intruder finding only; that is, IDS can detect attacks but cannot avoid or react. Formerly the attacks are identified; the IDSs raise an alarm to inform the controller to take action. There is two important classes of IDSs. One is rule-based IDS and the other is anomaly-based IDS (Ganapathy, S., *et al*., 2012; Northcutt, S. and J. Novak, 2002).

II. Related Work:

Hae Young Lee *et al*. (2010) presented a false data detection method that exploits a fuzzy rule-based system to verify the legitimacy of sensor simulation report. Many metrics are evaluated depending on the collected reports in the base station are used for the confirmation. Compared to the existing crisp-based detection solutions, this method reduced errors in the detection, thanks to approximate reasoning provided by fuzzy logic.

Gerrigagoitia *et al*. (2012) presents a latest IDS construction depends on status and hope of the various nodes of a network for decision-making and analysis of possible sources of malicious attacks.

Michael Riecker *et al*. (2014) proposed a lightweight, energy-efficient scheme that makes use of mobile agents to find intrusions depends on the energy consumption of the sensor nodes as a metric. A linear regression model was applied to predict the energy consumption. From the results, it was indicated so as to denial-of-service injuries, like a flooding, should be detected with high accuracy, while keeping the number of false-positives very low.

Pu Cheng *et al*. (2014) developed intrusion detection algorithm called a robust model for numerous attribute of sensor nodes using t-distribution in network environment. This model with an approximate parameter algorithm was exploited to detect malicious attackers precisely. This algorithm achieved high detection accuracy and low false alarm rate still while minimum sensor nodes are dangerous, and execute quickly with a lower computational cost.

Francesco Buccafurri *et al*. (2014) proposed the trust-based systems constitute to ensure security of distributed systems. In this work, a trust-based approach was discussed to make WSNs tolerant against attacks targeting their routing layer. It was shown that how such attacks are tolerated with low overhead in comparison to unprotected systems.

Mostaque Md and Morshedur Hassan *et al*. (2013) presented a few research papers regarding the foundations of intrusion detection systems, the methodologies with efficient fuzzy classifiers using genetic algorithm that are the focus of current development efforts and the solution of the issues of interruption identification scheme to present a real world view of intrusion detection.

Nabil *et al*. (2013) presented a survey on current Intrusion Detection Systems and some open research problems related to WSN security. In Anomaly-based Intrusion identification is lightweight in environment; though they create more false alarms. Signature-based IDSs are suitable for comparatively big-sized WSNs; though they have some expenses such as updating and inserting new signatures. In Cross layer IDSs are

Australian Journal of Basic and Applied Sciences, 10(16) November 2016, Pages: 305-313

frequently not optional for wireless infrastructure having resources limitations with high energy and calculation is required for exchanging multilayer parameters.

Wenchao Li *et al*. (2014) proposed a latest interruption identification scheme depends on n-intermediate neighbor classification algorithm in wireless sensor network. This system separated abnormal nodes from true nodes by observing their misbehaving characteristics, and to analyze parameter collection and mistake rate of interruption identification scheme. This system has achieved an efficient, rapid intrusion detection by enhancing the wireless ad hoc on-demand distance vector routing protocol.

Mueen Uddin *et al*. (2013) focused on the efficiency and performance of the signature-based multi- layer IDS using mobile agents. It then discussed the growth of a latest mark- based ID using mobile nodes. This system uses mobile agents to transfer rule based signatures from large complementary list to minimum mark list and then frequently revise those databases with new signatures detected.

Aikaterini and Christos *et al*. (2012) examined how to properly use classification methods in intrusion detection for MANETs. It was performed a thorough analysis of five well-known classifiers. It was investigated that how simple categorization versus cost-sensitive categorization affect routine, all in conditions of CE-classification error with terms of WCE-weighted error and how hyper- parameter tuning affects performance when new unknown attacks. The datasets covered a broad range of situation counting different intruder varieties, different stages of network speed and misbehaving action and end different data set gaps for the interruption identification scheme.

Farzaneh *et al*. (2012) proposed adaptive anomaly detection system has some advantages such as using few but efficient parameters to update, online adaptation, tangible improvement in accuracy compared with non-adaptive methods and almost online adaptation. This system consists of a number of fuzzy rules that each one has a prediction confidence ratio. Test records are classified by using this model. After that experiment classification outputs and metrics that are required for updating the discovery scheme are loaded in the Buffer for each process. The user checks experiment report to contain a before mentioned latency and sends these verified results to the fuzzy model tuner.

Shakshuki *et al*. (2013) developed Enhanced Adaptive Acknowledgement for defending against malicious attacks. It does not affect network performance. In this paper, author does not focus on reliable neighbor nodes to forward the packets. Neighbor recommendation is necessary to discover and maintain the route. In the proposed work, new certificate based intrusion detection system to achieve network reliability for communication.

The proposed work aims to attain balance between malicious attacks and network integrity in network. The analysis is taken from network simulator tool.

III. Proposed Intrusion Detection System:

A. Intrusion Detection Algorithm:

We proposed an intrusion detection algorithm for the detection of malicious behaviors in the WSN. A node which does not follow the exact behaviour is called as malicious nodes. This attack aims to modify the message or drop the message etc. The algorithm is developed based on the following modules.

Modules:

The modules are as follows:

- Cluster based routing establishment is accomplished with node reputation.
- Hope reference charge is worn to find misbehaving node.
- Neighbor node information will be updated to source node and destination node after completing each route maintenance process.
- Asymmetric key authentication and key distributed system are used to make public key available to all the nodes. Each node carries two keys namely public key and private key.
- Digest of message is created by one way hash function.

Cluster based routing establishment:

Cluster is formed based on reliable neighbor nodes, using trust vector value. It is derived from how much of packet information is successfully carried via neighbor nodes from source node to destination node. The packet integrity should be maintained through the entire route. Each node has routing table which contains packet information, packet id, cluster member id, node to node connectivity, neighbor coverage range, link quality etc. Based on high and medium trust vector value, the node is considered as a cluster head otherwise cluster member.

Trust Vector T_B^A is given by,

$$\frac{Outcoming\ delivered\ packets\ from\ node\ B - Packets\ sent\ from\ node\ B\ to\ A}{Incoming\ received\ packets\ from\ node\ B - Packets\ sent from\ node\ A\ to\ B} \quad (1)$$

After calculating trust vector value, each node chooses one node that has highest trust value, it is called trust authenticator. Then the trust authenticator becomes cluster head and the chooser is considered as cluster member node. If the chosen sensor node is already a member of another cluster region, a mobile node of high trust value is selected. In this way, the cluster region is formed.

Route establishment:

Route is established between the nodes based on link stability. For transmission range T_r, link stability L_{sb} between any two nodes overtime period t can be calculated by:

$$L_{sb} = \frac{T_r}{\sqrt{\left\{\left(p_1^{'} - p_2^{'}\right) + t\left(n_1\cos\theta_1 + n_2\cos\theta_2\right)\right\}^2 + \left\{\left(q_1^{'} - q_2^{'}\right) + t\left(n_1\sin\theta_1 + n_2\sin\theta_2\right)\right\}^2}} \quad (2)$$

L_{sb} is the link stability of individual links between any two nodes and for a path and it is same as the minimum link stability along the path. Once the stability is calculated, the route discovery process is initiated by means of flooding route request packet from source to destination. If any destination node replies with route reply within periodical time, stability rate is high otherwise it is low. Cluster head maintains the link stability status among all the cluster members to the destination. Whether any route having high stability rate that route is consider as first priority for packet transmission. All cluster members update route establishment status to cluster head based on link stability rate. In order to avoid link break or failure by means of malicious attackers, link stability is maintained among all cluster members and cluster head.

Clock based Fuzzy Intrusion Detection System:

In fuzzy logic, Decision trees concept is employed to find the intrusion in the network. These trees are powerful tools describes the classification and prediction of datasets. It occurs in the rules formation that is easier for human understanding and these rules are derived from the existing database tools. The accurateness of the data classification plays a vital role in security applications. The Entropy characterizes either purity or impurity of an arbitrary collection of examples. It is used to define the information gain precisely.

It is implemented using the attribute selection algorithm as explained as follows:

Step 1. Initialize the queue S with set values and the attribute set values.

Step 2. The following steps from 3 until step 7 are performed if the size of the stack is not null.

Step 3. Generate a set value which consists of the queue value with maximum support and is a subset of the queue value.

Step 4. Calculate the expected information and information gain. The set contains only positive and negative samples with their corresponding labels. The expected information is calculated as follows,

$$I\left(S_q\right) = \sum_{i=1}^{q} - p_i \log_2 p_i \quad (3)$$

Where, S is the total number of samples.

q is total classes

$p_i = S_i/S$

A feature F with values (f_1, f_2, …..f_w) is divided in to w training subsets (s_1….s_w) where S_k is the subset which holds the value f_j for F. The entropy of the selected feature is given as

$$E(F) = \sum_{k=1}^{q} \frac{S_{1k} + ... + S_{qk}}{S} * I(S_{1k} .....S_{qk}) \quad (4)$$

The information gain, Gain (F) of an attribute A that is related to the collection of examples S, it is defined as follows,

$$Gain(F) = I(s_1, s_2 .....s_c) - E(F) \quad (5)$$

Step 5. Choose the attributes with information gain values.

Step 6. If the attribute value does not belong to the subset R then R is the common values of R along with the attributes

Step 6.Example set of terms forms a set based on the examples or the attribute values.

Step 7. The cluster head performs the testing as follows, the cluster head computes the new arriving node weighted distance using the weights. Let $s_1, s_2, \ldots, s_k$ be the **n**-intermediate relay nodes of an entity a with weights $w_1, w_2, w_3, \ldots, w_k$. The weighted distance of these n-nearest neighbors the object is defined as $w_1d_1, w_2d_2, \ldots, w_kd_k$ where $d_1, d_2, \ldots, d_k$ are the normal Euclidean distances $d(a, s_i) = w_id_i$.
The average weighted distance is computed as,

$$\frac{1}{k} * \left(\sum_{i=1}^{k} \frac{w_i d_i}{\sum w_i} \right) \quad (6)$$

If the distance of newly arrived node >the weighted average distance then the cluster head provides the result as abnormal else normal. Let us consider a packet transmission from node P to node Q. When a route establishes between source and destination the packet transmission takes place. When node Q receives a data packet from node P then *Detect Clock* to *PRESENT CLOCK*, start the *Detect Clock*. Now node Q generates a certificate for node A such as $CPQ_{CRR} = [H(m)]PRQ$ and send it to node *P*. After that node *P* will calculate the *Clock To Receive* for this certificate and compare with the *Detect Clock* of node *Q*. If it is greater, then the node *P* discards the certificate. Otherwise node *P* verify the certificate with the help of node *Q*'s public key. Finally, *weighed distance* value is compared, if it is greater that a predetermined threshold value then we mark node as a malicious node. The malicious nodes are detected during packet forwarding phase using clock based certificate determination method.

C. Proposed packet ID:

Source ID	*Destination ID*	*Confirmation condition*	*Interruption finding*	*Route discovery*	*Clock based Fuzzy*
2	2	4	4	4	2

Fig. 1: Proposed Packet format

In figure1. FSIDS proposed packet ID is shown. Here the source node ID carries 2 bytes and destination node ID carries 2 bytes. Next filed is a third one is the confirmation that condition of the node. The confirmation condition denotes an efficient communication path for packet transmission is selected. In fourth field, interruption finding. To detect the intrusion successfully certain amount of packet transmitted sender node to receiver node. Packets have node characteristics, node ID etc. In fifth, the energy maintenance ratio is allotted to ensure minimum energy usage. The last filed *Clock based Fuzzy* to find intruder present in current routing path and obtain best routing scheme.

IV. Performance estimation:

A. Simulation setup and Metrics:

The proposed IDS is simulated with Network Simulator tool (NS 2.34). In our simulation, 101 sensor nodes move in a 1000 meter x 1000 meter square region for 100 seconds time for simulation. Consider all nodes moving separately with the same standard velocity. All nodes have the coverage range as 250 meters in simulation area. Traffic for simulation is Constant Bit Rate (CBR).

Our simulation settings and parameters are summarized in table 1

No. of Nodes	101
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	50 bytes
Mobility Model	Random Way Point
Protocol	LEACH

B. Performance of parameters:

Then estimating characteristics of wireless network, according to given parameters.

Detection Efficiency:

The amount of identifiedmisbehaving nodes to overall count of nodes.

End-to-End delay:

Packet delay is averaged over all broadcasting data packets among the source to destination node.

Packet Delivery Ratio:

Rate of the number of packets received effectively and amount of data packets broadcasted from sender node.

Network simulation reports are discussed in the next part. We compare our proposed scheme with SIDS (Mueen Uddin, *et al*., 2013),, SVM (Aikaterini Mitrokotsa, Christos Dimitrakakis, 2012), AAIDS (Farzaneh Geramiraz, *et al*., 2012) and EAACK (Krasimira Kapitanova Sang H. Son, Kyoung-Don Kang, 2011) in presence of malicious node environment.

C. Results:

Normal characteristics of nodes obey with wireless network that means the probability that a node acts good is predetermined. While a node perform well than minimum percent of the interactions, it is considered as a malicious node. The default percentage of intruders present is 22 % in network.

Primary research, then vary the no. of malicious nodes as 20, 30 up to 100.

Figure 2 shows the results of detection efficiency for the nodes 20, 30….100 scenarios. Clearly our scheme achieves more detection rate than the previous schemes, since cluster based routing. In this routing, link stability is maintained and malicious nodes are identified using the trust recommendation and clock based certificate determination. Therefore the vulnerability of malicious nodes are reduced.

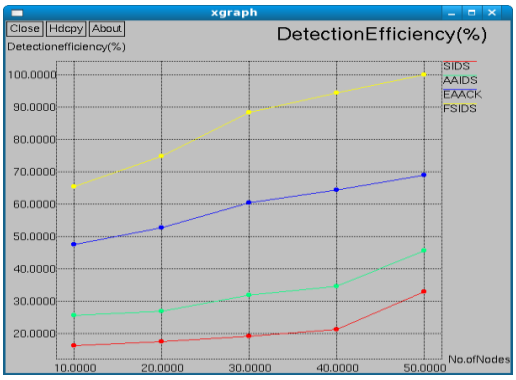

Fig. 2: No. of Nodes Vs Detection Efficiency

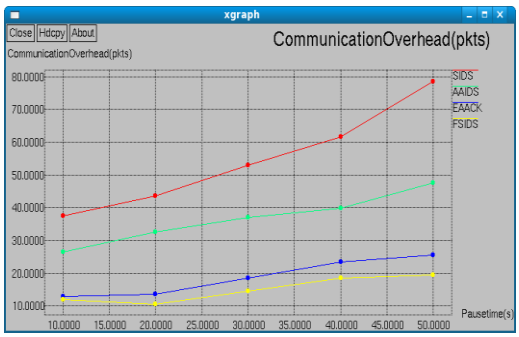

Fig. 3: Pause time Vs Communication Overhead

Figure 3 shows the results of Pause time Vs Communication overhead. From the results, we can see that proposed IDS achieves less overhead than previous schemes. It is because of link stability determination. Cluster head chooses only high stable link for data forwarding. So the network delivery rate is getting increased. Packet overhead will be suppressed because of link quality and reliability of neighbor nodes.

Figure 4 shows the results of packet delivery ratio for the speed. Clearly our system achieves more packet delivery ratio than previous intrusion detection systems. The proposed system comprises of two major aspects i.e. malicious detection and network authentication. Packet is delivered via reliable nodes through stable link. Successfully all the packets are delivered to the destination.

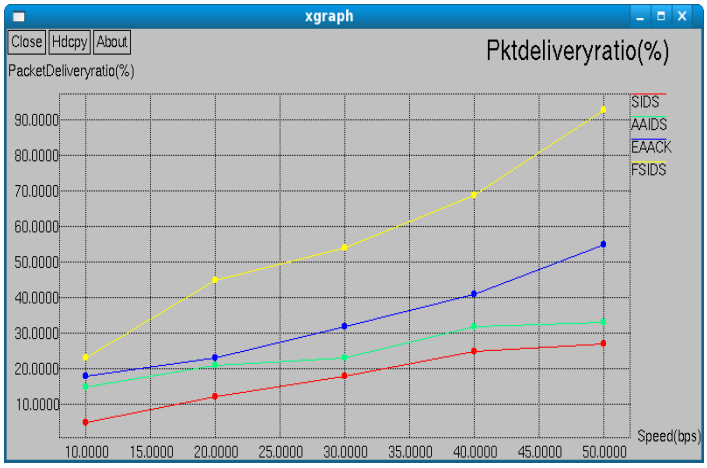

Fig. 4: Speed Vs Packet Delivery Ratio

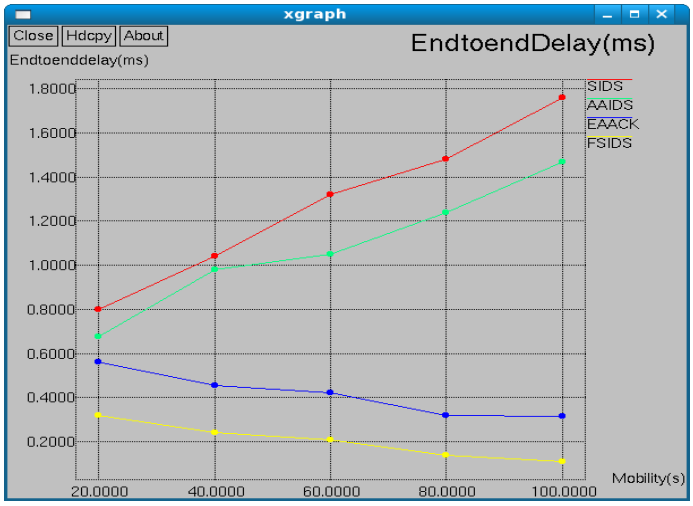

Fig. 5: Mobility Vs End to end delay

Figure 5 shows the results of Mobility Vs end to end delay. From the results, we can see that proposed system has less delay than previous systems. End to end delay should be kept minimize in order to satisfy QoS. The proposed system reduces delay by means of cluster based routing. Network partitioning will be reduced by integrating this routing in all networks.

Conclusion:

In WSN, it is easy to deploy the malicious nodes during packet transmission period. These attacks need to change the packet information, drops the packet and misroute the packets to wrong destination node. If it continues, network partitioning may likely to occur and it leads to network diconnectivity. Overcome this drawback, several intrusion detection systems were presented to detect malicious nodes with less false positive rate. In this proposed scheme, fuzzy based secure intrusion detection scheme is planned to make stability between authenticated nodes. The cluster routing path is established based on neighbor trust vector value to enhance packet transmission rate. If any node falls below the threshold value, it is considered as misbehaving node. Clock based fuzzy intrusion identification is also enhanced to identify intruders based on detection clock and weight based distance. If it reaches above the threshold value, intrusions can be detected fast. Fuzzy security system is also enhanced to provide data authentication and integrity, with minimum end to end delay. Based on the simulation results, the proposed scheme achieves a better performance than the existing schemes in terms of performance metrics.

REFERENCES

Aikaterini Mitrokotsa, Christos Dimitrakakis, 2012. Intrusion detection in MANET using classification algorithms: The effects of cost and model selection. Ad hoc Networks, Elseiver, pp: 1-12.

Baiah, C., M. Poonam, 2014. Intrusion Detection in Heterogeneous Wireless Sensor Networks with Liveliness Proficient Node Localization Algorithm. International Journal of Advanced Research in Computer and Communication Engineering, 3: 6.

Chia-Fen Hsieh, Rung-Ching Chen and Yung-Fa Huang, 2014. Applying an Ontology to a Patrol Intrusion Detection System for Wireless Sensor Networks. International Journal of Distributed Sensor Networks, Hindawi Publication, pp: 1-15.

Chong Eik Loo, Mun Yong Ng, Christopher Leckie and Marimuthu Palaniswami, 2006. Intrusion Detection for Routing Attacks in Sensor Networks. International Journal of Distributed Sensor Networks, 2: 313-332.

Francesco Buccafurri, Luigi Coppolino, Salvatore D'Antonio, Alessia Garofalo, Gianluca Lax, Antonino Nocera, Luigi Romano, 2014. Trust-Based Intrusion Tolerant Routing in Wireless Sensor Networks. Springer, 8666: 214-229.

Francisco Maciá-Pérez, Francisco J. Mora-Gimeno, Diego Marcos-Jorquera, Juan Antonio Gil-Martínez-Abarca,Héctor Ramos-Morillo, and Iren Lorenzo-Fonseca, 2011. Network Intrusion Detection System Embedded on a Smart Sensor. IEEE Transactions on Industrial Electronics, 58(3): 722-732.

Farzaneh Geramiraz, Amir Saman Memaripour, and Maghsoud Abbaspour, 2012. Adaptive Anomaly-Based Intrusion Detection System Using Fuzzy Controller. International Journal of Network Security, 14(6): 352-361.

Gulshan Kumar and Krishan Kumar, 2014. Design of an Evolutionary Approach for Intrusion Detection. The ScientificWorld Journal, pp: 1-15.

Ganapathy, S., P. Yogesh, and A. Kannan, 2012. Intelligent Agent-Based Intrusion Detection System Using Enhanced Multiclass SVM. Computational Intelligence and Neuroscience, pp: 1-11.

Gerrigagoitia, K., R. Uribeetxeberria, U. Zurutuza and I. Arenaza, 2012. Reputation based Intrusion Detection System for Wireless Sensor Networks", IEEE Communications on Complexity in Engineering, pp: 1-5.

Gope, P., T. Hwang, 2016. BSN-Care: A Secure IoT-based Modern Healthcare System Using Body Sensor Network. IEEE Sensors Journal, 16(5): 1368-1376.

Gope, P., T. Hwang, 2015. Untraceable Sensor Movement in Distributed IoT Infrastructure. IEEE Sensors Journal, 15(9): 5340-5348.

Hu, W., C.T. Chou, S. Jha and N. Bulusu, 2010. "Deploying Long- Lived and Cost-effective Hybrid Sensor Networks," Elsevier AdHoc Networks, 4(6): 749-767.

Hae Young Lee, Tae Ho Cho and Hyung-Jong Kim, 2010. Fuzzy-Based Detection of Injected False Data in Wireless Sensor Networks. Information Security and Assurance Communications in Computer and Information Science , Springer, 76: 128-137.

Khan, S., K. K. Loo and Z.U. Din, 2010. Framework for intrusion detection in IEEE 802.11 wireless mesh networks. International Arab Journal of Information Technology, 7(4): 435-440.

Khan, S., Jaime Lloret and Jonathan Loo, 2014. Intrusion Detection and Security Mechanisms for Wireless Sensor Networks. International Journal of Distributed Sensor Networks, Hindawi Publication, pp: 1-4.

Krasimira Kapitanova Sang H. Son, Kyoung-Don Kang, 2011. Using fuzzy logic for robust event detection in wireless sensor networks. Ad hoc Networks,Elsevier, pp: 1-14.

Lee, J.J., B. Krishnamachari, C.C.J. Kuo, 2010. Impact of Heterogeneous Deployment on Lifetime Sensing Coverage in Sensor Networks. IEEE, SECON.

Mueen Uddin, Azizah Abdul Rehman, Naeem Uddin, Jamshed Memon, Raed Alsaqour, and Suhail Kazi, 2013. Signature-based Multi-Layer Distributed Intrusion Detection System using Mobile Agents", International Journal of Network Security, 15(1): 79-87.

Michael Riecker, Sebastian Biedermann, Rachid El Bansarkhani and Matthias Hollick, 2014. Lightweight energy consumption-based intrusion detection system for wireless sensor networks. International Journal of Information Security, Springer, pp: 1-8.

Mostaque Md and Morshedur Hassan, 2013. Current Trends on Intrusion Detection System, Genetic algorithm and Fuzzy Logic", International Journal of Distributed and Parallel Systems, 4(2): 35-47.

Nguyen, T., A. Al-Saffar and E-N Huh, 2010. A dynamic ID-based authentication scheme. Proceedings of the Sixth International Conference on Networked Computing and Advanced Information Management (NCM), pp: 248-253.

Northcutt, S. and J. Novak, 2002. Network Intrusion Detection. SAMS, 3rd edition.

Nabil Ali Alrajeh, S. Khan and Bilal Shams, 2013. Intrusion Detection Systems in Wireless Sensor Networks: A Review. International Journal of Distributed Sensor Networks, 3: 1-7.

Pu Cheng, Minghua Zhu, Xianzhong Liu, 2014. Distributed T-Distribution-Based Intrusion Detection in Wireless Sensor Networks. Springer, 295: 313-323.

Srivastava, P.K., P. Rai, U. Singh, 2012. "Intrusion Detection: An Energy Efficient Approach in Heterogeneous WSN", International Journal of Scientific and Research Publications, 2: 11.

Shakshuki, E.M., Nan Kang, T.R. Sheltami, 2013. EAACK – A Secure Intrusion Detection System for MANETs. IEEE Transactions on Industrial Electronics, 60(3): 1089-1098.

Wenchao Li, Ping Yi, Yue Wu, Li Pan, and Jianhua Li, 2014. A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network. Journal of Electrical and Computer Engineering, Hindawi Publication, pp: 1-9.

Yang, D., S. Misra, X. Fang, G. Xue, J. Zhang, 2012. Two-tiered constrained relay node placement in wireless sensor networks: computational complexity and efficient approximations. IEEE Trans. Mobile Computing, 11(8): 1399-1411.