International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 3, March 2015
Available at http://internationaljournalofresearch.org

Survey on security in Wireless Sensor Networks

Mounica.M
M.E Network Engineering Department of Information Technology Velammal College of Engineering and Technology
Madurai, India.

S.Kamalesh M.E
Assistant Professor Department of Information Technology Velammal College of Engineering and Technology
Madurai, India

P.Ganesh Kumar
Professor Department of Information Technology KLN of Engineering and Technology
Madurai, India

Abstract—

Wireless Sensor Networks has wide range of applications. However the sensors have very limited processing power and lifetime. The sensors are deployed in unattended environments and they use radio frequency (RF) transmitter to communicate with other nodes. These nodes are compromised by the attackers. So the Provision must be made for secure communication for military applications which carry sensitive data. Power management and security are the major issues in WSN. The goal of this paper is to present a review on security solutions in use and their performance. We classify our paper into 4 sections. (i)Threats to WSN (ii)Security Solutions (iii)Intrusion detection.

Keywords:
WSN; Threats; WSN Security protocols; Data aggregation; attacks

I.INTRODUCTION

WSN is an emerging technology. It has wide range of applications. Its applications include health care, industries, military, warehouse etc. The sensor nodes are deployed in unattended environments. Wireless sensor networks are vulnerable to threats. An adversary can compromise a sensor node, alter the data, eavesdrop, inject fake messages, and waste network resource. We need to implement an efficient Security protocol and at the same time it should not consume more power.

The two important operations in sensor networks include

Data dissemination: the propagation of data/queries throughout the network. Data gathering: the collection of observed data from the individual sensor nodes to a sink.

II.SECURITY REQUIREMENTS

A wireless sensor network has same characteristics of a typical computer network. It exhibits many characteristics which are unique to it. The security services in a Wireless sensor networks should protect the information communicated over the network and the resources from attacks and misbehavior of nodes. The security requirements in WSN are

A. Data Confidentiality

Confidentiality refers to keep the information secret from unauthorized parties. In order to secure data from eavesdropper, it is necessary to ensure the confidentiality of sensed data. To achieve data confidentiality, encryption functions are normally used, which are a standard method and rely on a shared secret key existing between communicating parties.

To protect the confidentiality of data, encryption itself is not sufficient, as an eavesdropper can perform traffic analysis on the overheard cipher text, which could release sensitive information about the data.

B. Data Authenticity

Authentication is a process which enables a node to verify the origin of a packet and ensure data integrity. In WSNs an adversary is not just limited to modifying data packets. It can change the whole packet stream by injecting additional packets. The receiver node, therefore, needs to ensure that the

data used in any decision-making process originates from the correct sources .In many applications authentication is essential due to matters of sensitivity

C. Data Integrity

Data integrity issues in wireless networks are similar to those in wired networks. Data integrity ensures that any received data has not been altered or deleted in transit. We should keep in mind that an adversary can launch modification attacks when cryptographic checking mechanisms such as message authentication codes and hashes are not used. For example, A malicious node may add some fragments or alter the data within a packet. This new packet can then be sent to the original receiver

D. Data Freshness

Data freshness refers that the received messages are new, and previous messages are not replayed. Data freshness can be categorized into two types based on the message ordering: weak freshness, which provides only partial message ordering, but gives no information about delay and latency of the message. Strong freshness on other hand gives complete request-response pair and the delay information. Weak freshness is required by sensor measurements, while strong freshness is useful foretime synchronization within the network.

E. Data Availability

Providing availability requires that a sensor network should be functional throughout its lifetime. However, strict limitations and unnecessary overheads weaken the availability of sensors and sensor networks.

SECTION 1
III. SECURITY VULNERABILITIES IN WSN

Adversaries can Attacks at all the layers of network protocol. Resource limitations of WSN make these threats even more dangerous. WSN attacks are classified into two types

- Active attack: This attack affects the normal operation of the network. For eg: DOS attack

- Passive attack: It does not affect system operation but it learns information of the network. For eg: Traffic analysis

Wireless sensor networks attacks could be broadly considered from two different levels

- Attack against the security mechanism

- Attack against the basic mechanism (routing)

Denial of service (Dos): A Denial of Service attack in sensor networks is defined as any event that prevents the network's capacity to perform its desired function. DoS attacks in WSN may be carried out at different layers. This occurs by the unintentional failure of sensor nodes.Attacks on Physical layer include Jamming, Tampering and eavesdropping.

Jamming: The compromised node interferes with transmission and reception of data. It prevents the part of data from reaching receiver node. Tampering: It is also called as node capture. Adversaries gain full control over the sensor node through direct physical access. Eavesdropping: It is one of the Serious attack in WSN. The adversaries first monitor the network before performing any kind of attacks

Data link layer attacks include Exhausting and collision. Adversaries disobey the coordination rules and produce malicious traffic to interrupt network operations in the MAC layer.

Exhausting: The adversaries consume more energy Collision: Adversaries send bulk amount of data. Due to this the network lifetime decreases and also it consume more network resources causing collision in the network

Network layer attacks include Sybil attack, wormhole attack, sinkhole attack and hello flooding attack Sybil attack: In a Sybil attack, a node can take multiple identities which lead to the failure of the redundancy mechanisms of distributed data storage systems in peer-to peer networks. Sybil attack functions by its property of representing multiple nodes simultaneously. It is capable of damaging other fault tolerant schemes such as dispersity, voting, fair resource allocation and topology maintenance. This attack also affects geographical routing protocols, where the malicious node presents several identities to other nodes in the network thus appears to be in more than one location at a time. Location aware routing requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets. It is only reasonable to expect a node to accept but a single set of coordinates from each of its neighbors, but by using the Sybil attack an adversary can ‘‘be in more than one place at once’’.

Wormhole attack: Wormhole nodes fake a route that is shorter than the original one within the network; this can confuse routing mechanisms which rely on the knowledge about distance between nodes.It has one or more malicious nodes and a tunnel between them. The attacking node captures the packets from one location and transmits them to other distant located node which distributes them locally. A wormhole attack can easily be launched by the attacker without having knowledge of the network or compromising any legitimate nodes or cryptographic mechanisms.

Sinkhole attack: It prevents the base station from obtaining complete and correct sensing data. A compromised data tries to draw all or as much traffic as possible from a particular area by making itself attractive to the surrounding nodes and then do selective forwarding, modifying or eavesdrop packets

Hello flooding attack: New sensor node broadcasts “Hello” to find its neighbors and also it broadcast its route to the base station. It also validates that the node sending hello message is in the vicinity. Adversary can exploit this feature by using a high-powered wireless link. It can assure every node in the network that he is their neighbor, thus starting communication with nodes, As obvious by using this attack security of the information is compromised as the attacker gain access to the information flow in the network. Adversary should possess enough resources to manage this attack, and should be able to provide high quality routing path to other nodes in network. Traffic will find this path attractive enough to send packets through it, creating data congestion and disturbing the hierarchy of the data flow in network.

Transport layer attacks include flooding attack, inject false message and De-synchronization attack

Flooding attack: It is a DOS attack. The node Open many connections to overflow state buffer. It is designed to bring a network or service down by flooding it with large amounts of traffic. Once this buffer is full no connections can be made, and it results in Denial of Service.

False messages: Adversaries can inject false information by altering the correct data. De-synchronization attack: The attacker disrupts the active connection. It sends bogus sequence number or control flags

Application layer attacks include network programming attack and selective message forwarding Network programming attack: Nodes can be reprogrammed in the field.Adversaries can Attack by sending false program Selective message forwarding: In a multi hop network the compromised nodes selectively forwards data. It may also drop packets.

SECTION 2

V SECURITY MECHANISMS

According to Murad, Rassam, anazida zainal, in An Efficient Distributed Anomaly Detection Model for Wireless Sensor Networks[1] consists of two stages. In *Training stage* the normal observations are gathered at every sensor to find out the local normal model(LNM) and send it to the cluster head (CH) for constructing the global normal model (GNM).During *detection stage* Each node tests every observation using the GNM. The GNM model is composed of (*Max, Min)* values calculated at CH. Each observation is identified as either normal or anomalous by comparing with the detection thresholds specified in the GNM model. Performance is high. No communication overhead but it is efficient only in small sensor networks.

According to the author of Secure Data Aggregation with MAC Authentication in Wireless Sensor Networks [2] It is MAC based technique. It is simple and lightweight. As the number of nodes increases, the performance of cluster head decreases. Ko-ming Chang, yau hwang,mong-fong horng developed a new intrusion prevention and detection approaches for clustering based sensor networks [3]. It is MAC and LEACH based technique. Energy consumption is low. Here the drawbacks are sensor node cannot move. New nodes cannot be added. Miloud, Noureddine, Abdelraouf, Yacine proposed a protocol called SEDAN. (Secure and efficient protocol for data aggregation in wireless sensor networks) [4] A node uses initial key to generate pairwise key with its neighbour and each node erase its initial key. It is MAC based technique. It eliminates redundancy. Its energy is saved. When nodes are increased overhead also increases.

Intrusion Detection for Wireless Sensor Network Based on Traffic Prediction Model (SD) [5]. Author developed a technique based on Markov process in which the present state depends on past state. Initially the network is secure. The traffic pattern is compared periodically if it is abnormal it send alert to CH. No special techniques needed and low computational complexity. It detects only selective forwarding attacks and DOS attacks.

Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks [6]. In this process it is Hard to fool because the data used for detection is unique to its location. This paper focus only on temperature data

El-Sayed, El-Alfya, Feras N. Al-Obeidat developed a multi criterion fuzzy classification method with greedy attribute selection for anomaly-based intrusion detection [7]. The target here is to reduce the hypothesis search space (eliminate redundant data) and improve the performance. The authors analyzed the data with predefined patterns. In an rule based approach [8] the attribute selection module collects data and also selects necessary attributes based on information gain ratio value and the data's are classified using classifier. The decision maker decides whether the nodes send normal packets or malicious packets.

Stealthier attack on zone routing protocol in wireless sensor network [9] focus on Intra zone routing protocol and inter zone routing protocol. Overhead decreases and

Packet delay decreases. This paper focus only on sinkhole attack.

A non-cooperative game approach for intrusion detection in sensor networks [10] Here the Cluster is formed using LEACH mechanism and Non zero sum technique was proposed. If distance is the only criterion for cluster formation the number messages passing is higher.

According to Ilker Onat ,Ali Miri[11] each node Contains buffer. Initially packet length(arrive time and receive power) is stored and then compared with new incoming packets.(packet buffer length).Here More false alarms are generated due to variations in power.

A real time node based traffic anomaly detection algorithm for wireless sensor networks [12] Observe neighbour and built their profiles. When receiving packets their profiles are checked (profiles are stored in buffer. Edith C. H. Ngai, Jiangchuan Liu, and Michael R. Lyu, proposed intruder detection for sinkhole attack in wireless sensor networks [13]. The algorithm first lists the suspect nodes and efficiently identifies the intruder in the list through flow graph. It is effective and accurate. Higher energy consumption but it is accurate.

Quarter sphere based anomaly detection in wireless sensor networks [14] Contain parent node and children node. Each node runs intrusion detection algorithm. CN calculates its radius and send to PN. Parent node calculate global radius. This technique has lower detection rate.

Catching packet droppers and modifiers in wireless sensor networks [15] Here the nodes are arranged in tree structure. Parent node is sink. Each node adds extra info along either the packet. Sink analyze the packet for droppers and modifiers. Most Effective and has Low overhead in terms of communication and energy saving

Applying data mining techniques to intrusion detection in wireless sensor networks [16]. The author developed the Tree structure. It consists Local agent, Central agent. Both share messages to detect anomalies. Low energy consumption and accurate. Have reduced false positive rates.

An experimental study of hierarchical intrusion detection for wireless industrial sensor networks [17] Two hop clustering model are CH monitor nodes and nodes are divided to monitor CH. Consumes more energy

Okoli, Ejiro, Mona Evaluation of security problems and intrusion detection systems for routing attacks in wireless self-organized networks [18] Contains phenomenon nodes and it moves. Nodes observe PN and send periodic reports to CH

Anomaly detection based secure in-network aggregation for wireless sensor networks [19] Nodes monitor neighbour and compare it with them. They generate events if anomalies are detected.

A novel rule based intrusion detection framework for wireless sensor networks [20] It contains 3 phase: Local auditing, Rule application, Intrusion detection.

Dynamic multisource multipath routing is [21] Leach based. It performs geographic routing, Establish pairwise keys. The neighbor nodes gives votes to the target nodes.

An intrusion detection for cluster based wireless sensor networks [22] It collect behavior characteristic(certain parameters), measures deviation, compare with threshold, give weights, judgment.

Hierarchical energy efficient intrusion detection system for black hole attacks in WSN’s [23] Nodes send control packets to CH. CH analyze control packets. It is simple but energy is consumed.

A network lifetime enhancement method for sink relocation and its analysis in wireless sensor networks [24] Sink relocated based on capacity. Computational complexity. Systematic design of trust management systems for wireless sensor networks [25] Build trust. 4 components: Trust producer, manager, consumer, external manager. communication between them is bidirectional.

Agent based intrusion detection and self - recovery system for wireless sensor networks [26] It is agent based. Energy consumption is reduced. compromised node is recovered so now lifetime is increased.

Policy and network –based intrusion detection system for IPv6 enabled wireless sensor networks [27] Watchdogs(hids,nids) eavesdrop the exchanged messages between nodes and eventually compares. Computational burden is less.

Group based intrusion detection system in wireless sensor networks [28] Divide nodes into groups. Run ID algorithm in each groups. Alarm will be generated. Less false alarm. High detection rate.

A survey of intrusion detection [29] .Here the author deals with types of intrusion detection techniques.

A density-based fuzzy imperialist competitive clustering algorithm for intrusion detection in wireless sensor networks [30] Imperialist competitive algorithm. If one empire loses its power others will compete to take its place. It enhance detection and clustering accuracy.

Distributed anomaly detection [31]. This deals with local data partitioning, thresholds are introduced to classify data, its communicated to the next leave, further evaluation.

Signaling game theory strategy of intrusion detection in wireless sensor networks[32] If the record is malicious set up a game and defend. It has high detection rate, low false alarms, decreased power consumption.

The author of this paper [33] Introduced 3 concepts: Fuzzy system, reinforcement learning, multi agent system.

Cooperative game theoretic approach using fuzzy q-learning for detecting and preventing intrusion in wireless sensor networks [34] Combination of game theoretic approach and fuzzy algorithm.

Co-FAIS: cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks [35] Combination of game theoretic approach and fuzzy algorithm. High defense rate. High resistence to DOS attack. It cause congestion and downtime on WSN. It is complex.

Using fuzzy logic for robust event detection in wireless sensor networks [36] Fuzzification: convert crisp data into fuzzy data set. Decision making: convert them to if then rule. De-fuzzification: computes crisp result.

SECTION 3

VI INTRUSION DETECTION IN WSN

Solutions to security attacks [40] against networks involve three main components :

i) Prevention: It aims to prevent any attack before it happens. The proposed technique will have to defend against the targeted attack.

ii) Detection: If the intruder is able to pass the prevention step, then it is a failure to defend against the attack. At this Scenario, the security solution should switch into the detection phase. This step identify the nodes that are being compromised.

iii) Mitigation: It aims to mitigate any attack after it happens. Mitigation is the removal of the affected nodes and securing the network.

Intrusion is an unauthorized activity in a network that is either achieved passively or actively. In a security system, the first line of defense is Intrusion Prevention and the second line of defense is Intrusion Detection. It is the detection of any suspicious behavior in a network performed by the network members.

Intrusion Detection Systems (IDSs) provide some or all of the following information to the other supportive systems: identification of the intruder, location of the intruder, time of the intrusion, intrusion activity, intrusion type, layer where the intrusion happens.

CONCLUSION

This literature review briefly explains the threats and security solutions. Military applications need high level of security. Implementing security mechanism in resource constrained nodes reduces network lifetime. Therefore the security mechanism and energy should be optimized. However these researchers focus on compromised nodes. If the cluster head is compromised we need to secure the other part of the network. Our future work focus on compromised cluster head and optimizing energy

REFERENCES

[1.] Tae Ho Kim, Chang Hoon Kim, Chun Pyo Hong, and Hiecheol Kim," Comparison of Security Protocols for Wireless Sensor Networks"

[2.] Murad A.Rassam,anazida zainal,Mohd aizaini Marrof. "An efficient distributed anamaly detection model for wireless,"2013 AASRI Proceddings.

[3.] Soufiene Ben Othman,Abdelbasset Trad,Habib Youssef,Hani Alzaid. "Secure data aggregation with MAC authentication in Wireless Sensor Networks,2013 12th IEEE international Conference on trust,Security and privacy in computing and communications pp. 188-195

[4.] Ko-ming chang, Yau hwang,mong-fong horng." The new intrusion prevention and detection approaches for clustering-based sensor networks wireless sensor networks," Wireless Communications and Networking Conference, pp. 1927 - 1932 Vol. 4 2005 IEEE

[5.] Miloud Bagaa, Noureddine Lasla, Abdelraouf Ouadjaout, Yacine Challal," SEDAN: Secure and Efficient protocol for Data Aggregation in wireless sensor Networks,"2007 32nd IEEE Conference on Local Computer Networks

[6.] Han zhijie, wang Ruchuang," Intrusion detection for wireless sensor networks based on Traffic Prediction Model,",2012 International Conference on Solid State and Material Science pp. 1053-1060.

[7.] Sarjoun S. Doumit, Dharma P. Agrawal," Self organized criticality & stochastic learning based intrusion detection system for wireless sensor networks" Volume 25, 2012, pp. 2072–2080.

[8.] El-Sayed M. El-Alfya,, Feras N. Al-Obeidat," A multicriterion fuzzy classification method with greedy attribute selection for anomaly-based intrusion detection" The 9th International Conference on Future Networks and Communications" Volume 34, 2014, pp. 55–62.

[9.] K. Anand', S. Ganapathy, K. Kulothungan, P. Yogesh, A. Kannan," A rule based approach for attribute selection and intrusion detection in wireless sensor networks.," 2012 ELSEVIER Volume 38, 2012, pp. 1658–1664.

[10.] Arpit Chaudhari, Prachi Jaini," Stealthier Attack on Zone routing Protocol in Wireless Sensor Network", 2014 Fourth International Conference on Communication Systems and Network Technologies pp. 734-738.

[11.] Afrand Agah, Sajal K. Das and Kalyan Basu," A Non-cooperative Game Approach for Intrusion Detection in Sensor Networks", 2004 IEEE pp. 343-346

[12.] Ilker Onat ,Ali Miri" An Intrusion Detection System for Wireless Sensor Networks" in Proc. IEEE 2005, volume 3 pp.253-259.

[13.] Ilker Onat, Ali Miri," A Real-Time Node-Based Traffic Anomaly Detection Algorithm for Wireless Sensor Networks" Proceedings of the 2005 Systems Communications ,pp. 422-427.

[14.] Edith C. H. Ngai, Jiangchuan Liu, and Michael R. Lyu," On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks" IEEE ICC 2006 proceedings vol 8 pp. 8164-9547.

[15.] Sutharshan Rajasegarar, Christopher Leckie, Marimuthu Palaniswami, James C. Bezdek," Quarter Sphere Based Distributed Anomaly Detection in Wireless Sensor Networks", ICC 2007 proceedings pp. 3864-3869.

[16.] Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang, and Wensheng Zhang," Catching Packet Droppers and Modifiers in Wireless Sensor Networks" IEEE Secon 2009 proceedings vol 23 Issue 5 pp 835-843.

[17.] Coppolino L,D'Antonio, S.garofolo, Romano L,"Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks", 3PGCIC Eighth International Conference 2013 pp.247-254.

[18.] Sooyeon Shin, Taekyoung Kwon, Gil-Yong Jo, Youngman Park, and Haekyu Rhy," An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks", IEEE Transactions On Industrial Informatics, VOL. 6, 2010

[19.] Okoli Adaobi, Ejiro Igbesoko, Mona Ghassemian," Evaluation of Security Problems and Intrusion Detection Systems for Routing Attacks in Wireless Self-organised Networks", in Proc IEEE 2012

[20.] Bo Sun, Xuemei Shan, Kui Wu, and Yang Xiao," Anomaly Detection Based Secure In-Network Aggregation for Wireless Sensor Networks", IEEE Systems Journal, VOL. 7, MARCH 2013 pp. 13-25.

[21.] Ms. T. Eswari, Dr. V. Vanitha," A novel Rule Based Intrusion Detection Framework for Wireless Sensor Networks". 2013 International Conference on Information Communication and Embedded Systems pp.1019-1022.

[22.] Hamid Al-Hamadi and Ing-Ray Chen," Dynamic Multisource Multipath Routing for Intrusion Tolerance and Lifetime Maximization of Autonomous Wireless Sensor Networks," IEEE Eleventh International Symposium on Autonomous Decentralized Systems 2013 pp 1-7.

[23.] XueDeng," An Intrusion Detection System for Cluster Based Wireless Sensor Networks",2013 NICT.

[24.] Samir Athmani1, Djallel Eddine Boubiche2 and Azeddine Bilami," Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs", in Proc IEEE Computer and Information Technology 2013 pp.1-5.

[25.] Chu-Fu Wang, Jau-Der Shih, Bo-Han Pan, and Tin-Yu Wu," A Network Lifetime Enhancement Method for Sink Relocation and Its Analysis in Wireless Sensor Networks", IEEE Sensors Journal, Vol. 14, 2014.

[26.] P. Raghu Vamsi and Krishna Kant," Systematic Design of Trust Management Systems for Wireless Sensor Networks: A Review", 2014 Fourth International Conference on Advanced Computing & Communication Technologies.

[27.] Ting SUN, Xingchuan LIU," Agent based intrusion detection and self-recovery system for wireless sensor networks", 2013 5th IEEE International Conference on Broadband Network & Multimedia Technology ,pp.206-210.

[28.] João P. Amaral1, Luís M. Oliveira, Joel J. P. C. Rodrigues, Guangjie Han4, Lei Shu," Policy and Network-based Intrusion Detection System for IPv6-enabled Wireless Sensor Networks" IEEE ICC 2014 - Communications Software, Services and Multimedia Applications Symposium pp.1796-1801.

[29.] Guorui Li a,, Jingsha He , Yingfang Fu," Group-based intrusion detection system in wireless sensor networks",Science Direct Computer Communications (2008) Volume 31, Issue 18, 18 December 2008, Pages 4324–4332

[30.] Robert Mitchell, Ing-Ray Chen," A survey of intrusion detection in wireless network applications", Science Direct Computer Communications (2014)

[31.] Shahaboddin Shamshirband a,b,⇑, Amineh Amini c, Nor Badrul Anuar b, Miss Laiha Mat Kiah b,Ying Wah Teh c, Steven Furnell," D-FICCA: A density-based fuzzy imperialist competitive clustering algorithm for intrusion detection in wireless sensor networks", ELSEVIER Vol 55,2014, Pages 212–226

[32.] Heshan Kumaragea,∗, Ibrahim Khalil a, Zahir Tari a, Albert Zomaya," Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modelling", Journal of Parallel and Distributed Computing, vol 73, Issue 6,2013 pp. 790-806

[33.] Shigen Shena,b, Yuanjie Li a, Hongyun Xua, Qiying Cao," Signaling game based strategy of intrusion detection in wireless sensor networks",ELSEVIER Computers and Mathematics with Applications 2011,pp. 2404-2416.

[34.] ShahaboddinShamshirband a,b,n, NorBadrulAnuar a,b, MissLaihaMatKiah a,b, AhmedPatel," An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique", ELSEVIER Engineering ApplicationsofArtificial Intelligence 2013 pp. 2105-2127.

[35.] Shahaboddin Shamshirband a,b,n, AhmedPatel c,d, NorBadrulAnuar b, Miss LaihaMatKiah b, AjithAbraham," Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks", ELSEVIER Engineering Applications of Artificial Intelligence vol 32,2014 pp.228-241.

[36.] Shahaboddin Shamshirband, NorBadrulAnuar, MissLaihaMatKiah, Vala AliRohani, Dalibor Petković, Sanjay Misra, Abdulnasirkhan," Co-FAIS: Cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks", ELSEVIER Journal of Network and Computer Applications,vol 42, 2014 pp.102-117.

[37.] Krasimira Kapitanova a,, Sang H. Son a, Kyoung-Don Kang ," Using fuzzy logic for robust event detection in wireless sensor networks" ELSEVIER Ad-hoc networks,vol 10, 2012, pp.709-722.

[38.] Shun-Sheng Wang, Kuo-Qin Yan , Shu-Ching Wang , Chia-Wei Liu," An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks", ELSEVIER Expert Systems with Applications, vol 38, 2011,pp.15234-15243.

[39.] Miao Xie, SongHan , BimingTian,SaziaParvin,” Anomaly detection in wireless sensor networks: A survey”, ELSEVIER Journal of Network and Computer Applications 2011, vol 34,pp. 1302-1325

[40.] Hung-Jen Liao a, Chun-HungRichardLin , Ying-ChihLin , Kuang-YuanTung,” Intrusion detection system: A comprehensive review”, ELSEVIER Journal of Network and Computer Applications 2013,vol 36, pp.16-24.

[41.] H.H. Soliman , Noha A. Hikal , Nehal A. Sakr,” A comparative performance evaluation of intrusion detection techniques for hierarchical wireless sensor networks”, Egyptian Informatics Journal 2012,vol 13,pp.225-238.

[42.] Quazi Mamun, Rafiqul Islam, Mohammed Kaosar,” Establishing Secured Communications in Cluster based Wireless Sensor Networks,2013 International Symposium on Wireless and Pervasive Computing pp. 1-6.

[43.] Pengfei H, Kai Xing, Xiuzhen Cheng Hao Wei, Haojin Zhu,” Information Leaks Out: Attacks and Countermeasures on Compressive Data Gathering in Wireless Sensor Networks”, 2014 - IEEE Conference on Computer Communications pp.1258-1266.

[44.] Triana Mugia Rahayu, Sang-Gon Lee, Hoon-Jae Lee,” Security analysis of secure data aggregation protocols in wireless sensor networks” ICACT 2014.

[45.] Josna Jose, Joyce Jose, Fijo Jose,” A Survey on Secure Data Aggregation Protocols in Wireless Sensor Networks” International Journal of Computer Applications 2012