"IDS FOR WIRELESS SENSOR NETWORK : A REVIEW"

Rakesh Sharma
Department of Computer Science
CRM Jat College, Hisar
rakeshsharma3112@gmail.com

***Abstract*— Wireless sensor network typically consists of large number of low-cost densely deployed sensor nodes that have strictly constrained sensing, computation, and communication capabilities. Because of resource restricted sensor nodes, it is necessary to reduce the amount of information transmission so that average lifetime of sensor and thus the bandwidth consumption are improved. As wireless sensor networks are typically deployed in remote and hostile environments to transmit sensitive data, sensor nodes are in danger of node compromise attacks and security issues like data confidentiality and integrity are terribly necessary. Therefore, in this paper we have explored general security threats in wireless sensor network and made an extensive study to categorize available data gathering protocols and analyze possible security threats on them.**

I. INTRODUCTION

Due to the recent advancement in Micro-Electro-Mechanical Systems (MEMS), wireless communication like Bluetooth [1], IEEE 802.11 [2], or Mobile Ad-hoc Networks (MANETs) [3], a new concept of networking known as Wireless Sensor Networks (WSNs) has emerged. The definition from SmartDust program of Defense Advanced Research Project Agencies (DARPA) is: "A sensor network is a deployment of massive numbers of small, inexpensive, self-powered devices that can sense, compute, and communicate with other devices for the purpose of gathering local information to make global decisions about a physical environment" [4]. Wireless Sensor Network, consists of large number of sensor nodes having the capability of wireless communication, limited computation and sensing. WSN was initially developed for military and disaster rescue purposes but because of the availability of ISM band (2.4 GHz), the technology is now emerging in public applications also. The salient feature in Wireless Sensor Network makes it different from other network; self-organize, low power, low memory, low bandwidth for communication, large-scale nodes, self-configurable, wireless, infrastructure-less. Therefore, WSN design must encounter these features in order to provide a reliable network. However each sensor node is equipped with its own sensor, processor and radio transceiver, so it has the ability of sensing, data processing and communicating with each other. WSN are relies on collaborative work of large number of sensor, for this reason, they are deployed densely throughout the area where they monitor specific phenomena and communicate with each other and with one or more sink nodes that interact with a remote user. The user can inject commands into the sensor network via the sink to assign data collection; data processing and data transfer tasks to the sensors in order to receive the data sensed by the network.

II. WIRELESS SENSOR NETWORK MODEL

Unlike their ancestor ad-hoc networks, WSNs are resource limited, they are deployed densely, they are prone to failures, the number of nodes in WSNs is several orders higher than that of ad hoc networks, WSN network topology is constantly changing, WSNs use broadcast communication mediums and finally sensor nodes don't have a global identification tags [5]. The major components of a typical sensor network are:

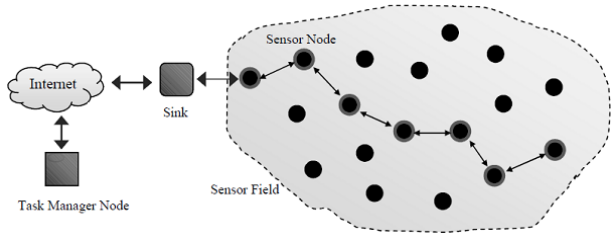

Fig.1. Components of Wireless sensor Networks

A. Sensor Field

A sensor field can be considered as the area in which the nodes are placed.

B. Sensor Nodes

Sensors nodes are the heart of the network. They are in charge of collecting data and routing this information back to a sink.

C. Sink

A sink is a sensor node with the specific task of receiving, processing and storing data from the other sensor nodes. They serve to reduce the total number of messages that need to be sent, hence reducing the overall energy requirements of the network. The network usually assigns such points dynamically. Regular nodes can also be considered as sinks if they delay outgoing messages until they have aggregated enough sensed information. Sinks are also known as data aggregation points.

D. Task Manager

The task manager also known as base station is a centralized point of control within the network, which extracts information from the network and disseminates control information back into the network. It also serves as a gateway to other networks, a powerful data processing and storage centre and an access point for a human interface. The base station is either a laptop or a workstation. Data is streamed to these workstations either via the internet, wireless channels, satellite etc. So hundreds to several thousand nodes are deployed throughout a sensor field to create a wireless multi-hop network. Nodes can use wireless communication media such as infrared, radio, optical media or Bluetooth for their communications. The transmission range of the nodes varies according to the communication protocol is use.

III. VULNERABILITIES AND CHALLENGES OF WSNS

WSNs are vulnerable against many kinds of attacks; some of the most common reasons are:

A. Theft [6] (reengineering and replicating) [7, 8].
B. Limited capabilities and resources [8,9].
C. Random deployment [10].
D. Deployment on dynamic/hostile environments [9,11].
E. Insider attackers.
F. Inapplicable traditional network's common security techniques [8,9] (due to limited devices and their re-sources and interaction to physical environment).
G. Requirement to redesigning security architectures and protocols (distributed and self-organized).
H. Unreliable communications [9] (connectionless packet-based routing unreliable transfer, channel's broadcast nature conflicts, multi-hop routing and network congestion and node processing Latency).
I. Vulnerability against eavesdropping (since using unique communication frequency into the WSN).
J. Unattended nature and operation [6,9].
K. Dynamic structure, unpredictable topology and self- organization [6.7].
L. Sensor nodes selfishness [9,12].
M. Requiring to forwarding and routing sensed information to a shared destination, called sink.
N. Existence redundancy in gathered traffic.
O. Fault tolerant [6,12].
P. Cost of sensor nodes development and their production [9,13].
Q. Size and precision of sensor nodes.

IV. SECURITY IN WSNs

As WSNs' application areas are growing, intrusion techniques in these networks also are increasing; there are many methods to disrupt these networks and every day, new techniques are representing to destruct WSNs [6,9]. Besides, in attending to the vital WSNs' vulnerability against many types of attacks [8,14] and necessity of data accuracy and network health and fault tolerant, confidential and sensitive applications of WSNs, security is a vital requirement in these networks and it must be established according to their constraints to can solve security problems and weaknesses of these networks. Also, there are three security key points on WSNs, including system (integrity, availability), source (authentication, authorization) and data (integrity, confidentiality). Thus, security in WSNs is an important, critical issue, necessity and vital requirement, due to:

- Correctness of network functionality [6,9].
- Unusable typical networks protocols [9,10].
- Limited resources and un-trusted sensor nodes [6,15].
- Requiring trusted center for key management, to authenticate nodes to each others, preventing from existent attacks and selfishness [6,11,16] and extending collaboration [9].
- Broadcast and wireless nature of transmission media [6,8].
- Sensor nodes deploy on hostile environments [6,12,13] (unsafe physically).
- Unattended nature and operation of WSNs [8,9,17].

V. ATTACKS AGAINST SENSOR NETWORKS

Due to the lack of tamper-resistant packaging and the insecure nature of wireless communication channels, these networks are vulnerable to internal and external attacks. WSN are prone to failure and malicious user attack because it is physically weak, a normal node is very easy to be captured to become a malicious node or by inserting a malicious node in the network [6,7,10,11,12,16].

A. Spoofed, altered, or replayed routing info

This attack targets the routing info changed between the nodes. Adversaries is also able to produce routing loops, attract or repel network traffic, extend or shorten supply routes, generate false error messages, partition the network, and increase end-to-end latency. The quality answer for this attack is authentication. i.e., routers can solely settle for routing info from valid routers.

B. Selective forwarding attack

In a multi-hop mode of communication a malicious node could refuse to forward sure messages and easily drop them, making certain that they are not propagated any longer

C. Sinkhole attack

By sinkhole attack, somebody tries to draw in nearly all the traffic from a specific space through a

compromised node. A compromised node that is placed at the centre of some space creates an outsized "sphere of influence", attracting all traffic destined for a base station from the sensor nodes. The assailant targets an area to make depression wherever it will attract the foremost traffic, presumably nearer to the bottom station so the malicious node might be perceived as a base station.

D. Sybil attack

Most protocols assume that nodes have one distinctive identity within the network. In a very Sybil attack, an assailant will seem to be in multiple places at identical time. This may be convincing by making faux identities of nodes settled at the sting of communication vary. Multiple identities may be occupied inside the sensor network either by fabricating or stealing the identities of legitimate nodes.

E. Wormholes attack

In this attack somebody might win over nodes agency would unremarkably be multiple hops from a base station that they are just one or two hops away via the hole. The best case of this attack is to possess a malicious node forwarding information between two legitimate nodes. Wormholes usually win over distant nodes that they are neighbors', resulting in fast exhaustion of their energy resources.

F. Hello flood attack

Many protocols need nodes to broadcast hello packets for neighbor discovery, and a node receiving such a packet could assume that it is inside (normal) radio vary of the sender. A laptop-class assailant with giant transmission power might win over each node within the network that somebody is its neighbor, so all the nodes can answer the hello message and waste their energy. The results of a hello flood are that each node thinks the assailant is inside one-hop radio communication vary.

G. Information integrity attack

Data integrity attacks compromise the information travelling among the nodes in WSN by ever-changing the information contained inside the packets or injecting false data. The assailant node should have a lot of process, memory and energy than the sensor nodes. The goals of this attack are to falsify sensor information and by doing thus compromise the victim's analysis

H. Energy drain attack

Fancied reports can cause false alarms that waste world response efforts, and drain the finite quantity of energy in a very battery high-powered network. But the attack is feasible provided that the intruder's node has enough energy to transmit packets at a relentless rate. The aim of this attack is to destroy the sensor nodes within the network, degrade performance of the network and ultimately split the network grid and consequently lead of a part of the sensor network by inserting a brand new Sink node.

I. Black-hole attack

The part attack positions a node in vary of the sink and attracts the complete traffic to be routed through it by advertising itself because the shortest route. Somebody drops packets returning from specific sources within the network.

J. Node replication attack

This is an attack wherever assailant tries to mount many nodes with same identity at totally different places of the prevailing network.

VI. INTRUSION DETECTION SYSTEM (IDS)

Intrusion Detection System in simple term is the system or say hardware/software which can detect or prevent the system from insider and outsider attacks in which it is placed. To prevent or detect network infrastructure from web threats, cybercrimes, and of course from internal attacks Intrusion Detection System has been proven to be the most important intrusion detection tool. Intrusion detection system proved to be a major tool which is used for network administrator to defend networks from threats, worms, and insider attacks. An Intrusion detection system (IDS) has been proposed for years as a most effective security measure. For intrusion detection purpose basic two traditional IDS techniques are used: i) Signature Based IDS and ii) Anomaly Based IDS [19].

A. Ids Classification Based On Detection Method

1) Signature based IDS

Signature based IDS also termed as Misuse based IDS. In this type of intrusion detection technique predefined dataset/pattern which is generally called as signature provided by the system. This predefined data set has been generated by the security experts. In Signature based Intrusion Detection System (SIDS) can detect known attacks through matching signature in predefined attack pattern. Unfortunately, this technique is capable to identify only known and predefined patterned attacks. The Major drawback of this technique is that they are unable to catch totally new malicious activity or say unknown threats. Though, their execution of identification is extremely high. Thus, it comes to the new technique of IDS (i.e. Anomaly based IDS). These signatures are composed of several elements which are defined by network traffic. For example SNORT. In signature based IDS tools like SNORT and BRO is used.

2) Anomaly based IDS

To monitor system's behavior the techniques used are Anomaly based IDS (AIDS). Suppose, one pattern which is predefined which comes through the network traffic during the communication between two or more than that, at this time pattern changed or say intruder attacks on that which cannot identify by the signature based IDS. But when it is used anomaly based IDS it checks the whole behaviour of out coming packets as well as insider packets. If it founds any kinds of behavioural changes in that it will deny the packet and send it to log and then send it to the reporting system. This technique overcomes the issue related to detect unknown and abnormal behavioural activities. But by using this technique system gets high false alarm rate. Various machine learning and data mining techniques/algorithms used in anomaly detection techniques

3) Hybrid IDS

Hybrid IDSs are a combination of both anomaly-based and signature-based approaches. Hybrid mechanisms usually contain two detection modules; that is, one module is responsible of detecting well-known attacks using signatures, while the other is responsible for detecting and learning normal and malicious patterns or monitor network behavior deviation from normal profile.

B. Ids Categorization Based On Their Architecture

Intrusion Detection Systems (IDSs) attending to the information gathering source and input data supplier [18], divide into three categories, as follows.

4) Host-Based Intrusion Detection System (HIDS)

HIDS installs on a computer system; it uses processor and memory of that system and protects only the hosting system. It has an abnormal detector part which using statistical methods to detect abnormal behavior of users in comparison to their behavioral records; also, it has an expert system part that detects the security threats and describes the vulnerabilities of the system, but independent from behavioral records of users; of course, it uses a rules-base, too.

5) Network-Based Intrusion Detection System (NIDS)

NIDS is a software process which installs on a special hardware system; in many cases, it operates as a sniffer and controls passing packets and active communications, then it analyzes network traffic in sophisticated, to find attacks NIDS can identify at-tacks, on network level.

6) Distributed Intrusion Detection System (DIDS).

- Most important characteristics of DIDS are:
- Combination of HIDS, NIDS and central management system;
- Sending the reports of distributed IDSs (HIDSs and NIDSs) to the central management system;
- Based on distributed and heterogeneous resources ;
- High complexity, variable specifications and agent- based.

In WSNs, most attackers are targeting routing layer, since they can control passing information into the network. Besides, WSNs mainly are based on sensor nodes' reporting to the base station; so, disrupting and violating from this process leads to success attacks. As a result, for such networks, most proper architecture for IDS will be NIDS. A NIDS using network raw data packets as data source; it eavesdrops and listens to the network traffic, captures packets in real-time, then controls and tests them to detect attacks. There is a SIDS on each sensor node to detect attacks on sensor-level wide; mainly, physical attacks. Also, in the proposed architecture, sensor nodes are partitioned as some clusters; each cluster has a cluster-head and any cluster-head (CIDS) should monitor the traffic of its associated cluster nodes. But, in some cases (about boundary nodes), a single cluster-head cannot solve the "trust no node" requirement; thus, neighboring and corresponding cluster-heads have to cooperate to each others to complete the intrusion detection process. They can use the simple majority vote rule to make an appropriate decision. In other cases, a human agent or the WSNIDS (deployed IDS on the central server) is completing the intrusion detection process.

VI. LITERATURE REVIEW

A. Signature based intrusion detection system

Signature based IDS, also known as rule-based IDS, has predefined rules of different security attacks. When the network's behaviour shows any deviation from the predefined rules, it is classified as an attack.

A specification based decentralized security mechanism is proposed by A. P. R. Da Silva et al., that is well known in the research field of intrusion detection systems for wireless sensor networks[20]. It works in three phases; data acquisition, rule application and intrusion detection. During rule application phase, monitor node applies rules for various attacks such as exhaustion attack, selective forwarding, black hole attack and flooding attack etc.

An ant-colony-based IDS in conjunction with machine learning is another rule-based IDS proposed by S. Banerjee et al. [21]. The proposed IDS perceive behavior and acts using self-organizing principle initiated with probability values.

Roman et al introduce a neighbour monitoring technique called spontaneous watchdog [22]. They favor specification based detection scheme for WSNs over other detection techniques. This architecture consists of local and global agents; however it is not implemented yet.

Intrusion Detection Program (IDP) is proposed by A. Abraham et al, which is capable to detect known attacks [23]. IDP is based on genetic programming (GP) technique and is effective against a variety of attacks such as denial of service (DoS) and unauthorized access. IDA uses three variants of GP such as linear genetic programming (LGP), multi expression programming (MEP), and gene-expression programming (GEP). GEP and MEP detection and classification accuracy are greater than 95%.

A distributed IDS (DIDS) using soft computing techniques is presented by A. Abraham et al. [24]. It uses few fuzzy rule-based classifiers to identify intrusions. The authors claim that fuzzy classifier provides 100% accuracy for all kinds of intrusions.

A rule-based IDS for WSNs is presented by I. Krontiris et al[25] . It is host based in which every node has IDS. The architecture of the proposed IDS has many modules such as packet monitoring, cooperative engine, detection engine, and response unit. The IDS is basically designed for routing attacks and is capable of detecting packet-dropping attacks.

An IDS for detection of sink-hole attack is presented by I. Krontiris et. al.[26]. The proposed IDS are hosted on each sensor node and require TinyOS with the combination of MintRoute routing protocol. It is an advanced version of [25] with narrow approach; that is, the former can detect many packet-dropping and misdirecting attacks while the latter is only designed for detection of sink-hole attacks. In both approaches, every node monitors and cooperates with neighbors.

Intrusion Detection Architecture (IDA) is presented by H. Jadidoleslamy [27]. IDA is distributed and hierarchical in nature which can operate by cooperation of sensor nodes, cluster head, and central system. IDA generates either passive or active response on the basis of attack nature. However, this work does not present results on the detection rate and false positive and false negative ratios.

B. Anomaly based intrusion detection system

Anomaly based IDS monitors network activities and classifies them as either normal or malicious using heuristic approach. Most of anomaly-based IDSs identify intrusions using threshold values; that is, any activity below a threshold is normal, while any condition above a threshold is classified as an intrusion.

A sliding window based IDS using threshold value is efficient in the detection of few security attacks such as route depletion attacks is given by] I. Onat et al.[28].

A set of intrusion detection techniques at different layers is presented by V. Bhuse [29]. These techniques are independent of each other. At physical layer, RSSI values are used to detect masquerade, while at network layer, a specialized table driven routing protocol is used to detect routing and authentication attacks.

A cluster based IDS for routing attack is proposed by C. E. Loo et al [30]. This mechanism is capable of building a normal traffic model, which is used to differentiate between normal and abnormal traffic. The normal traffic model consists of number of packets received and sent, number of route requests received and sent, and so forth. The IDS can detect many attacks such as periodic route error attack and sink-hole attack.

An unsupervised neural network based IDS by Y. Y. Li et al [31] are capable of learning and detecting unknown attacks. This intelligent system learns the time-related changes using Markov model. When any intrusion occurs, a mobile agent moves to the malicious region of the WSN to investigate. The proposed mechanism can detect time-related changes and events.

The main advantage of anomaly-based IDS is its capability to detect new and unknown attacks; however sometimes it fails to detect even well-known security attacks. Many anomalies based IDSs have been proposed so far [32].

C. Hybrid Intrusion Detection System

Hybrid IDSs are a combination of both anomaly-based and signature-based approaches.

A hierarchical hybrid IDS for detection of routing attacks is presented by T. H. Hai et al. [33]. It has high accuracy in terms of detection of network layer security attacks such as sink hole and worm hole.

A cluster based hybrid IDS is given by K. Q. Yan et al. [34], where the cluster head is responsible for detecting intrusions. The key idea behind this mechanism is to reduce energy consumption.

A further enhanced IDS is proposed by K. Q. Yan et al. [35]. The enhanced IDS have three modules, that is, anomaly-based detection, signature-based detection, and decision making. A supervised back propagation network is used to learn and identify normal and malicious packets.

A hybrid intrusion detection model is presented by M. S. I. Mamun et al. [36]. In this model, sensor nodes are divided into hexagonal regions like cellular networks. Each region is monitored by a cluster node, while cluster nodes are monitored by regional nodes. The base station has the responsibility to monitor all regional nodes. It is hierarchical in nature forming a tree-like structure. Attack signatures are stored in base station and propagated toward the leaf node for attack detection. Similarly the mechanism has predefined specifications of normal and abnormal behaviour. Anomaly detection is done by measuring deviation from defined specifications. The authors did not

mention detection rate or false-alarm ratio of their proposed mechanism. Furthermore, it is not clear which security attacks are detected using this mechanism.

Another hybrid IDS using support vector machine (SVM) and misuse detection is proposed by H. Sedjelmac et al. [37]. A distributed learning algorithm is used to train SVM to distinguish normal and malicious patterns. This intrusion detection mechanism is designed to operate in cluster based WSNs, where all nodes monitor their neighbours. The authors claim high detection rate with fewer false positives; however attack types are not described.

An IDS that uses state transition analysis and stream flow to detect sync-flood attack against WSNs is presented by R. Bhatnagar et al. [38]. This mechanism monitors three way handshake of TCP to identify attack pattern; however it is not yet implemented and tested.

REFERENCES

[1] Chatschik Bisdikian, "An overview of the Bluetooth wireless technology", IEEE Communication Magazine, vol. 39, no. 12, December 2001, pp. 86-94.

[2] Brain P. Crow, Indra Widjaja, Jeon Geun Kim and Prescott T. Sakai, "IEEE 802.11 Wireless Local Area Networks", IEEE Communication Magazine, Vol. 35, Sep 1997, pp 116-126

[3] Corson, J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, Jan 1999.

[4] Stephan Olariu, "Information assurance in wireless sensor networks", Sensor network research group, Old Dominion University, in proceeding of: 19th International Parallel and Distributed Processing Symposium (IPDPS 2005), Denver, CO, USA, Jan2005,

[5] Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks", In Mobile Computing and Networking, 2000, pp. 243–254.

[6] Mohammadi, R. A. Ebrahimi and H. Jadidoleslamy, "A Comparison of Routing Attacks on Wireless Sensor Networks," International Journal of Information Assur-ance and Security, Vol. 6, No. 3, 2011, pp. 195-215.

[7] Mohammadi and H. Jadidoleslamy, "A Comparison of Transport and Application Layers Attacks on Wireless Sensor Networks," International Journal of Information Assurance and Security, Vol. 6, 2011, pp. 331-345.

[8] Sharma and M. K. Ghose, "Wireless Sensor Networks: An Overview on Its Security Threats," International Journal of Computers and Their Applications, Vol. 1, Special Issue on "Mobile Ad-hoc Networks", 2010, pp. 42-45.

[9] S. Mohammadi and H. Jadidoleslamy, "A Comparison of Link Layer Attacks on Wireless Sensor Networks," In-ternational Journal of Information Security, Vol. 2, No. 2, 2011, pp. 69-84.

[10] Saxena, "Security in Wireless Sensor Networks: A Layer-based Classification," Department of Computer Science, Purdue University, 2011 .https:/ /www.cerias. purdue.edu/apps/ reports_a nd _papers/view/3106

[11] Z. Li and G. Gong, "A Survey on Security in Wireless Sensor Networks," Department of Electrical and Com-puter Engineering, University of Waterloo, Canada, 2011. http://www.cacr.math.uwaterloo.ca/techreports/2008/cacr200 8-20.pdf

[12] Dimitrievski, V. Pejovska and D. Davcev, "Security Issues and Approaches in WSN, Department of computer science," Faculty of Electrical Engineering and Informa-tion Technology, Skopje, 2011. http://ict-act.org/ICTInntions... /ictinnovations 2009 _sub missi on_ 21.pdf

[13] S. Mohammadi and H. Jadidoleslamy, "A Comparison of Physical Attacks on Wireless Sensor Networks," Interna-tional Journal of Peer to Peer Networks, Vol. 2, No. 2, 2011, pp. 24-42.

[14] J. Yick, B. Mukherjee and D. Ghosal, "Wireless Sensor Network Survey," Elsevier's Computer Networks, Vol. 52, No. 12, 2008, pp. 2292-2330.

[15] A. Zia, "A Security Framework for Wireless Sensor Networks," Doctor of Philosophy (PhD) Thesis, The School of Information Technologies, University of Syd-ney, 2008.

[16] Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Pro-ceedings of the 1st IEEE International Workshop on Sen-sor Network Protocols and Applications, Alaska, 11 May 2003, pp. 113-127.

[17] Perrig, R. Szewczyk, V. Wen, D. Culler and D. Tygar, "SPINS: Security Protocols for Sensor Networks," Pro-ceedings of 7th Annual International Conference on Mo-bile Computing and Networks, Rome, July 2001.

[18] S. Mohammadi and H. Jadidoleslamy, " A High-Level Architecture for Intrusion Detection on Heterogeneous Wireless Sensor Networks: Hierarchical, Scalable and Dynamic Reconfigurable," Interna-tional Journal Wireless Sensor Network, 2011, 3, 241-261doi:10.4236/wsn.2011.37026 Published Online July 2011 (http://www. SciRP.org /journal/wsn)

[19] Nabil Ali Alrajeh, S. Khan, and Bilal Shams "Intrusion Detection Systems in Wireless Sensor Networks: A Review" International Journal of Distributed Sensor Networks ,Volume 2013, 7 pages

[20] P. R. Da Silva, A. A. F. Loureiro, M. H. T. Martins, L. B. Ruiz, B. P. S. Rocha, and H. C.Wong, "Decentralized intrusion detection in wireless sensor networks," in Proceedings of the 1st ACMInternationalWorkshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet '05), pp. 16–23, Montreal, Canada, October 2005.

[21] S. Banerjee, C. Grosan, and A. Abraham, "IDEAS: Intrusion detection based on emotional ants for sensors," in Proceedings of the 5th International Conference on Intelligent Systems Design and Applications (ISDA '05), pp. 344–349, September 2005.

[22] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," in Proceedings of the 3rd IEEE Consumer Communications and Networking Conference (CCNC '06), pp. 640–644, January 2006.

[23] Abraham, C. Grosan, and C. Martin-Vide, "Evolutionary design of intrusion detection programs," International Journal of Network Security, vol. 4, no. 3, pp. 328–339, 2007.

[24] Abraham, R. Jain, J. Thomas, and S. Y. Han, "D-SCIDS: distributed soft computing intrusion detection system," Journal of Network and Computer Applications, vol. 30, no. 1, pp. 81–98, 2007.

[25] Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in Proceedings of the 13th EuropeanWireless Conference, Paris, France,April 2007.

[26] Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of Sinkhole attacks in wireless sensor International Journal of Distributed Sensor Networks 7 networks," in Algorithmic Aspects of Wireless Sensor Networks ALGOSENSORS, vol. 4837 of LectureNotes in Computer Science, pp. 150–161, Springer, 2008.

[27] Jadidoleslamy, "A hierarchical intrusion detection architecture for wireless sensor networks," International Journal of Network Security & Its Applications, vol. 3, no. 5, 2011.
[28] Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '2005), pp. 253–259, August 2005.
[29] Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," Journal of High Speed Networks, vol. 15, no. 1, pp. 33–51, 2006.
[30] E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami, "Intrusion detection for routing attacks in sensor networks," International Journal of Distributed Sensor Networks, vol. 2, no. 4, pp. 313–332,2006.
[31] Y. Y. Li and L. E. Parker, "Intruder detection using a wireless sensor network with an intelligent mobile robot response," in IEEE Conference Southeastcon, pp. 37–42, April 2008.
[32] S. Islam and S. A. Rahman, "Anomaly intrusion detection system in wireless sensor networks: security threats and existing approaches," International Journal of Advanced Sciences andTechnology, vol. 36, pp. 1–8, 2011.
[33] T. H. Hai, F. Khan, and E. N. Huh, "Hybrid intrusion detection system for wireless sensor networks," in Computational Science and Its Applications—ICCSA 2007, vol. 4706 of Lecture Notes in Computer Science, pp. 383–396, Springer, Berlin, Germany, 2007.
[34] Q. Yan, S. C. Wang, and C. W. Liu, "A hybrid intrusion detection system of cluster-based wireless sensor networks," in Proceedings of the International Multi-Conference of Engineers and Computer Scientists (IMECS '09), Hong Kong, 2009.
[35] Q. Yan, S. C. Wang, S. S. Wang, and C. W. Liu, "Hybrid Intrusion Detection System for enhancing the security of a cluster-based Wireless Sensor Network," in Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT '10), pp. 114–118, Chengdu, China, July 2010.
[36] S. I. Mamun and A. F. M. Sultanul Kabir, "Hierarchical design based intrusion detection system for wireless ad hoc sensor network," International Journal of Network Security & Its Applications, vol. 2, no. 3, 2010.
[37] Sedjelmaci andM. Feham, "Novel hybrid intrusion detection system for clustered wireless sensor network," International Journal of Network Security & Its Applications, vol. 3, no. 4, 2011.
[38] R. Bhatnagar and U. Shankar, "The proposal of hybrid intrusion detection for defense of sync flood attack in wireless sensor network," International Journal of Computer Science & Engineering Survey, vol. 3, no. 2, pp. 31–38, 2012.