Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 167575, 7 pages
http://dx.doi.org/10.1155/2013/167575

Research Article

Intrusion Detection Systems in Wireless Sensor Networks: A Review

Nabil Ali Alrajeh,[1] S. Khan,[2] and Bilal Shams[2]

[1] *Biomedical Technology Department, College of Applied Medical Sciences, King Saud University, Riyadh 11633, Saudi Arabia*
[2] *Institute of Information Technology, Kohat University of Science and Technology (KUST), Kohat City 26000, Pakistan*

Correspondence should be addressed to Nabil Ali Alrajeh; nabil@ksu.edu.sa

Received 28 February 2013; Accepted 16 April 2013

Academic Editor: Jaime Lloret

Wireless Sensor Networks (WSNs) consist of sensor nodes deployed in a manner to collect information about surrounding environment. Their distributed nature, multihop data forwarding, and open wireless medium are the factors that make WSNs highly vulnerable to security attacks at various levels. Intrusion Detection Systems (IDSs) can play an important role in detecting and preventing security attacks. This paper presents current Intrusion Detection Systems and some open research problems related to WSN security.

1. Introduction

Wireless Sensor Networks (WSNs) are composed of sensor nodes and sinks. Sensor nodes have the capability of self-healing and self-organizing. They are decentralized and distributed in nature where communication takes place via multihop intermediate nodes. The main objective of a sensor node is to collect information from its surrounding environment and transmit it to the sink. WSNs have many applications and are used in scenarios such as detecting climate changed, monitoring environments and habitats, and various other surveillance and military applications. Mostly sensor nodes are used in such areas where wired networks are impossible to be deployed. WSNs are deployed in physical harsh and hostile environments where nodes are always exposed to physical security risks damages. Furthermore, self-organizing nature, low battery power supply, limited bandwidth support, distributed operations using open wireless medium, multihop traffic forwarding, and dependency on other nodes are such characteristics of sensor networks that expose it to many security attacks at all layers of the OSI model.

Many security-related solutions for WSNs have been proposed such as authentication, key exchange, and secure routing or security mechanisms for specific attacks. These security mechanisms are capable of ensuring security at some level; however they cannot eliminate most of the security attacks [1]. An IDS is one possible solution to address a wide range of security attacks in WSNs.

An IDS is also referred to as a second line of defence, which is used for intrusion detection only; that is, IDS can detect attacks but cannot prevent or respond. Once the attack is detected, the IDSs raise an alarm to inform the controller to take action. There are two important classes of IDSs. One is rule-based IDS and the other is anomaly-based IDS [2, 3]. Rule-based IDS is also known as signature-based IDS which is used to detect intrusions with the help of built-in signatures. Rule-based IDS can detect well-known attacks with great accuracy, but it is unable to detect new attacks for which the signatures are not present in intrusion database. Anomaly-based IDSs detect intrusion by matching traffic patterns or resource utilizations. Although anomaly based IDSs have the ability to detect both well-known and new attacks, they have more false positive and false negative alarms. Some IDSs operate in specific scenarios or with particular routing protocols. Watchers [4] operate with proactive routing protocol to detect routing anomalies. It is implemented on each node, so all the nodes need some sort of cooperation to detect routing intrusions. Some intrusion detection mechanisms also operate with reactive routing protocols [5, 6]. These

mechanisms enable the network to select a reliable path from source to destination.

This paper presents a review of existing IDSs. It is organized as follows. In Section 2, we examine existing security attacks. In Section 3, we analyze and discuss some already proposed IDSs. We make comparison of existing IDSs on the basis of detection. In Section 4, we highlight some open research issues and directions, and finally in Section 5, we conclude the paper.

2. Overview of Security in Wireless Sensor Networks

WSNs are vulnerable to many types of security attacks due to open wireless medium, multihop decentralized communication, and deployment in hostile and physically nonprotected areas. Different threat models are discussed in [7] such as mote-class attacks and laptop-class attacks. In mote-class attacks, the attacker compromises few of the sensor nodes inside a WSN. In laptop-class attacks, the attacker has more powerful device(s) to launch more intense attack against WSNs.

Security attacks against WSNs can be classified as active and passive [8–10]. Passive attacks are silent in nature and are conducted to extract important information from the network. Passive attacks do not harm the network or network resources. Active attacks are used to misdirect, temper, or drop packets. The unique characteristics such as wireless medium, contention-based medium access, multihop nature, decentralized architecture, and random deployment of such networks make them more vulnerable to security attacks at various layers.

Physical layer of WSN is responsible for radio and signals management. Radio jamming is one of the severe attacks against WSN [8, 11]. Another physical layer attack is battery exhaustion attack. In a WSN, battery power of sensor nodes plays an important role and determines the lifetime of the network. Keeping in view the power limitations of WSNs, it is highly desirable to design power efficient mechanisms for sustainable WSNs. Sensor nodes in sleep mode consume less energy as compared to active mode. In energy exhaustion attack, the attacker tries not to allow sensor nodes to switch to sleep mode. This can be done by sending unnecessary data or beacons to sensor nodes to keep them always busy. As WSNs are deployed in hostile environment, it is susceptible to many physical attacks such as node destruction, node replacement, node replication, battery replacement, or reprogramming of node with malicious code [12, 13]. However such attacks need to physically access the network.

Most WSNs use contention based carrier sense multiple access with collision avoidance mechanism (CSMA/CA). This mechanism tries to avoid collision; however it adds more complications in the form of collision, hidden-node problem, MAC selfishness, and unfairness [7, 8]. Possible countermeasures against such kind of attacks are small frames and rate limitations [7, 14].

Network layer is responsible for appropriate route selection from source to destination [15, 16]. In WSN, the multihop route from source to destination is vulnerable to many active and passive attacks [17, 18]. Active attacks include packet-dropping attacks, packet-misdirecting attacks, rushing attack, Sybil attack, byzantine attack, routing table overflow attack, spoofed routing information, hello flood, and acknowledgement spoofing [8, 19].

3. Intrusion Detection Systems

One of the key features of a WSN is its multihop distributed operations, which add more complexity in terms of security attack detection and prevention. In a multihop distributed environment, it is very difficult to locate attackers or malicious nodes. Many security attack detection and prevention mechanisms are designed for WSNs; however most of the existing solutions are capable of handling only a few security attacks. For example, most secure routing protocols are designed to counter few security attacks [20, 21]. Similarly new media access mechanisms are designed to handle hidden-node problem or selfishness. Encryption mechanisms are designed to protect data against passive attacks. Hence, one can say that there is a need to design mechanisms that are capable enough of detecting and preventing multiple security attacks in WSNs. An Intrusion Detection System (IDS) is one possible solution to it.

An intrusion is basically any sort of unlawful activity which is carried out by attackers to harm network resources or sensor nodes. An IDS is a mechanism to detect such unlawful or malicious activities [22]. The primary functions of IDS are to monitor users' activities and network behaviour at different layers.

A single perfect defence is neither feasible nor possible in wireless networks, as there always exist some architectural weaknesses, software bugs, or design flaws which may be compromised by intruders. The best practice to secure wireless networks is to implement multilines of security mechanisms; that is why IDS is more critical in wireless networks. It is viewed as a passive defence, as it is not intended to prevent attacks; instead it alerts network administrators about possible attacks well in time to stop or reduce the impact of the attack. The accuracy of intrusion detection is generally measured in terms of false positives (false alarms) and false negatives (attacks not detected), where the IDSs attempt to minimize both these terms [3].

There are two important classes of IDSs. One is known as signature-based IDS, where the signatures of different security attacks are maintained in a database. This kind of IDS is effective against well-known security attacks. However, new attacks are difficult to be detected as their signatures would not be present in the database. The second type is anomaly-based IDS. This kind is effective to detect new attacks; however it sometimes misses to detect well-known security attacks. The reason is that anomaly-based IDSs do not maintain any database, but they continuously monitor traffic patterns or system activities.

IDS can operate in many modes, for example, standalone operation and cooperative cluster based operation [23]. A standalone IDS operates on every node to detect

unwanted activities. Cooperative cluster based IDS are mostly distributed in nature in which every node monitors its neighbours and surrounding nodes activities and operation; in case of any malicious activity detection, the cluster head is informed.

Broadly speaking, IDS has three main components [3] as shown in Figure 1.

(i) Monitoring component is used for local events monitoring as well as neighbours monitoring. This component mostly monitors traffic patterns, internal events, and resource utilization [24].

(ii) Analysis and detection module is the main component which is based on modeling algorithm. Network operations, behavior, and activities are analyzed, and decisions are made to declare them as malicious or not.

(iii) Alarm component is a response generating component, which generates an alarm in case of detection of an intrusion.

It should be noted that IDSs are passive in nature and can only detect intrusion. They cannot take any preventive action; they only generate an alarm. It is then the administrator's job to take preventive measures against the attack. Researchers in WSNs are working on two broad categories of IDSs, that is, signature-based and anomaly-based IDSs.

3.1. Signature-Based Intrusion Detection Systems. 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. Signature-based IDSs are well suited for known intrusions; however they cannot detect new security attacks or those attacks having no predefined rules [3]. In this section, we present existing signature-based IDSs for WSNs.

In [25], a rule-based IDS for WSNs is presented. 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 in [26]. The proposed IDS is hosted on each sensor node and requires 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 neighbours. Intrusion Detection Architecture (IDA) is presented in [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.

In [28], Intrusion Detection Program (IDP) is proposed, which is capable to detect known attacks. 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), multiexpression 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 in [29]. It uses few fuzzy rule-based classifiers to identify intrusions. The authors claim that fuzzy classifier provides 100% accuracy for all kinds of intrusions.

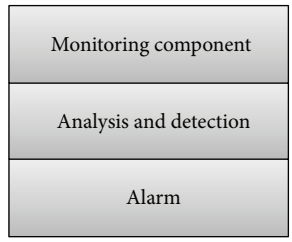

Figure 1: Components of IDS.

A decentralized rule-based IDS is proposed in [30]. This mechanism has three main phases, namely, data acquisition, rule application, and intrusion detection. The proposed mechanism is capable of detecting many routing attacks such as worm-hole, black-hole, selective-forwarding, and delay attacks. The authors also claim that the proposed solution is capable of detecting jamming attack as well; however they did not explain how jamming attacks are detected as it is a physical layer attack. Spontaneous watchdog IDS and its basic architecture is given in [31]. This architecture consists of local and global agents; however it is not implemented yet. An ant-colony-based IDS in conjunction with machine learning [32] is another rule-based IDS. The proposed IDS perceives behaviour and acts using self-organizing principle initiated with probability values. Different signature-based IDSs are given in Table 1.

3.2. Anomaly-Based Intrusion Detection Systems. 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. 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 anomaly-based IDSs have been proposed so far [33]. An unsupervised neural network based IDS [34] is 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.

A set of intrusion detection techniques at different layers is presented [35]. 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

Table 1: Signature based IDSs.

IDS	Mechanism	Attacks	Evaluation metrics
[25]	Collaborative	Black hole, selective forwarding	Window length, false negative rates
[26]	Local and cooperative detection	Sink hole	Detection rate, false negative rates
[27]	Hierarchical	N/A	N/A
[28]	Genetic programming	DoS, unauthorized access	Classification accuracy
[29]	Soft computing	Unauthorized access, probing	Classification accuracy
[30]	Specification based	Repetition attack, delay attack, worm hole, alteration attack, black hole, selective forwarding	Detection rate, false positives
[31]	Spontaneous watchdog	N/A	N/A
[32]	Ant colony	Abnormal transmission	N/A

Table 2: Anomaly based IDSs.

IDS	Mechanism	Attacks
[34]	Artificial neural network	Time related changes
[35]	Set of techniques at OSI layers	Masquerade, routing attacks
[36]	Cluster based	Periodic route error attack, sink hole attack
[37]	Support vector	Black-hole attacks
[38]	Cross feature	Packet dropping attacks
[39]	Sliding window	Route depletion attack

Table 3: Hybrid IDSs.

IDS	Mechanism	Attacks
[40]	Hybrid, hierarchical	N/A
[41]	Support vector machine	N/A
[42]	State transition	Sync flood
[43]	Cluster based	Routing attacks
[44]	Cluster based, supervised learning, misuse detection	Routing attacks
[45]	Hierarchical and hybrid	Sink hole, worm hole

attacks. A cluster based IDS for routing attack is proposed [36]. 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. A support vector machine based IDS [37] is used to detect routing attacks such as black hole. It is basically cooperation based detection in which nodes communicate and share information about security attacks. A cross feature based anomaly detection mechanism is proposed in [38]. This mechanism monitors and learns normal traffic patterns in order to detect any intrusion in case of deviation. The IDS is capable of detecting packet-dropping and misdirecting attacks. A sliding window based IDS using threshold value is efficient in the detection of few security attacks such as route depletion attacks [39]. Table 2 presents a summary of a number of anomaly-based IDSs.

3.3. Hybrid Intrusion Detection Systems. 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. Hybrid IDSs are more accurate in terms of attack detection with less number of false positives. However, such mechanisms consume more energy and more resources. Hybrid IDSs are generally not recommended for a resource constraint networks such as a WSN; however they are still an active research area. A hybrid intrusion detection model is presented in [40]. 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 in [41]. 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 in [42]. This mechanism monitors three-way handshake of TCP to identify attack pattern; however it is not yet implemented and tested. A cluster based hybrid

Table 4: Comparison of different IDSs.

Characteristics	Anomaly based IDS	Signature based IDS	Hybrid IDS	Cross layer IDS
Detection rate	Medium	Medium	High	High
False alarm	Medium	Medium	Low	Low
Computation	Low	Low	Medium	High
Energy consumption	Low	Low	Medium	High
Attack detection	Few	Few	More	More
Multilayer attack detections	No	No	No	Yes
Strength	Capable of detecting new attacks	Detects all those attacks having signatures	Can detect both existing and new attacks	Can detect multilayer attacks
Weakness	Misses well known attack	Cannot detect new attacks	Requires more computation and resources	Requires more resources
Suitable for WSN	Yes	Yes	With justification	With strong justification

IDS is given in [43], 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 in [44]. The enhanced IDS has 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. Another hierarchical hybrid IDS for detection of routing attacks is presented in [45]. It has high accuracy in terms of detection of network layer security attacks such as sink hole and worm hole. Table 3 presents a summary of a few hybrid IDSs.

3.4. Cross Layer Intrusion Detection Systems. Cross layer design is a relatively new security technique in which different parameters across OSI layers are exchanged for optimal solutions [46]. Traditional IDS operates at a single layer of the OSI model and hence can monitor and detect intrusions at that particular layer. For example, network layer Intrusion Detection System can detect only routing attacks but cannot respond to MAC, physical, or transport layer anomalies. Cross layer IDSs have the capability to monitor and detect intrusions at multiple layers by communicating and exchanging parameters amongst different layers using cross layer interface. As we know, WSNs have many constraints in terms of computations, memory, and energy. Although cross layer IDS can detect many intrusions at different layers, this technique consumes more energy and computational resources by monitoring, analyzing, and exchanging multilayer parameters.

Cross layer intrusion detection agent (CLIDA) for WSNs is proposed in [47]. CLIDA ensures cross layer information exchange amongst physical, MAC, and network layer. Cross layer data module collects and represents data to all layers. CLIDA is capable of detecting multi-layer security attacks. This architecture has good detection rate; however energy and computational comparison is not given, which could be more interesting. Another cross layer security mechanism for WSN is proposed in [48], in which the authors have the observations that such mechanism would exhaust the limited resources of sensor nodes. In [24], a real-time cross layer security mechanisms for large scale flood detection and attack trace-back mechanism is presented. It uses different parameters from MAC and network layers to detect multilayer flooding attacks. It maintains different profiles for low, medium, and high intensity attacks.

4. Comparison and Discussion

Wireless Sensor Networks are distributed in nature using the multihop communication model. These networks are usually deployed in such areas where direct human interaction is either impossible or very difficult. Furthermore, WSNs have limitations in terms of computation, bandwidth, memory, and energy. These limitations are considered while designing any proposal for such networks. Due to the hostile environments of WSNs, security is one of their most important aspects. IDSs are widely used for securing WSNs. IDS has the ability to detect an intrusion and raise an alarm for appropriate action. Due to the energy and computational power limitations, designing appropriate IDS for WSN is a challenging task.

Anomaly-based IDSs are suitable for small-sized WSNs where few nodes communicate with the base station. In small sized WSNs, the traffic pattern is mostly the same, so unusual traffic pattern or changing behaviour can be treated as an intrusion. However such IDS may generate more false alarms and may not be able to detect well-known intrusions. Anomaly-based IDSs are usually lightweight in nature and mostly use statistical, probabilistic, traffic analysis or intelligent techniques.

Signature-based IDSs are suitable for relatively large-sized WSNs, where more security threats and attacks can compromise network operations. Signature-based IDS needs more resources and computations as compared to anomaly-based IDS. One of the important and complex activities is the compilation and insertion of new attack signatures in the databases. Such IDSs mostly use data mining or pattern matching techniques.

Hybrid IDSs are suitable for large and sustainable WSNs. These IDSs have both anomaly-based and signature-based modules, so they require more resources and computations.

To reduce the usage of limited resources, such mechanisms are mostly used in cluster based or hierarchical WSNs, in which some parts of the network are used to execute anomaly detection while other parts are accompanied with signature-based detection.

Cross layer IDSs are usually not recommended for a resource constraint networks such as WSNs, as it consumes more resources by exchanging parameters across the protocol suits for attack detection. Table 4 gives the comparison and characteristics of different IDSs.

5. Conclusions

While designing a security mechanism, we must consider the limited resources of WSNs. Anomaly-based IDSs are lightweight in nature; however they create more false alarms. Signature-based IDSs are suitable for relatively large-sized WSNs; however they have some overheads such as updating and inserting new signatures. Cross layer IDSs are usually not recommended for networks having resources limitations, as more energy and computation are required for exchanging multilayer parameters.

Acknowledgments

The authors extend their appreciation to the Research Centre, College of Applied Medical Sciences, and the Deanship of Scientific Research at King Saud University for funding this research.

References

[1] Y. Ping, J. Xinghao, W. Yue, and L. Ning, "Distributed intrusion detection for mobile ad hoc networks," *Journal of Systems Engineering and Electronics*, vol. 19, no. 4, pp. 851–859, 2008.

[2] S. Northcutt and J. Novak, *Network Intrusion Detection*, SAMS, 3rd edition, 2002.

[3] S. Khan, K. K. Loo, and Z. U. Din, "Framework for intrusion detection in IEEE 802.11 wireless mesh networks," *International Arab Journal of Information Technology*, vol. 7, no. 4, pp. 435–440, 2010.

[4] T. M. Chen, G.-S. Kuo, Z.-P. Li, and G.-M. Zhu, "Intrusion detection in wireless mesh networks," in *Security in Wireless Mesh Networks*, Y. Zhang, J. Zheng, and H. Hu, Eds., CRC Press, New York, NY, USA, 2007.

[5] M. K. Rafsanjani, A. Movaghar, and F. Koroupi, "Investigating intrusion detection systems in MANET and comparing IDSs for detecting misbehaving nodes," in *Proceedings of World Academy of Science, Engineering and Technology*, vol. 34, October 2008.

[6] E. J. Caballero, "Vulnerabilities of intrusion detection systems in mobile ad-hoc networks—the routing problem," in *TKK T-110.5290 Seminar on Network Security*, 2006.

[7] T. Roosta, S. Shieh, and S. Sastry, "Taxonomy of security attacks in sensor networks," in *Proceedings of the 1st IEEE International Conference on System Integration and Reliability Improvements*, vol. 1, pp. 529–536, Hanoi, Vietnam, 2006.

[8] S. Khan, N. Mast, and J. Loo, "Denial of service attacks and mitigation techniques in IEEE 802.11 Wireless mesh networks," *Information*, vol. 12, pp. 1–8, 2009.

[9] S. Khan and J. Loo, "Cross layer secure and resource-aware on-demand routing protocol for hybrid wireless mesh networks," *Wireless Personal Communications*, vol. 62, no. 1, pp. 201–214, 2010.

[10] S. Khan, N. Mast, K.-K. Loo, and A. Silahuddin, "Passive security threats and consequences in IEEE 802.11 wireless mesh networks," *International Journal of Digital Content Technology and Its Applications*, vol. 2, no. 3, pp. 4–8, 2008.

[11] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 38–43, 2004.

[12] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *International Journal of Computer Science and Information Security*, vol. 4, no. 2, 2009.

[13] S. Mohammadi and H. Jadidoleslamy, "A comparison of physical attacks on wireless sensor networks," *International Journal of Peer to Peer Networks*, vol. 2, no. 2, pp. 24–42, 2011.

[14] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[15] M. Hussaini, H. Bello-Salau, A. Salami, F. Anwar, A. Abdalla, and M. Islam, "Enhanced clustering routing protocol for power-efficient gathering in wireless sensor network," *International Journal of Communication Networks and Information Security*, vol. 4, pp. 18–28, 2012.

[16] A. Popescu, G. Tudorache, B. Peng, and A. Kemp, "Surveying position based routing protocols for wireless sensor and ad-hoc networks," *International Journal of Communication Networks and Information Security*, vol. 4, pp. 41–67, 2012.

[17] O. Fdili, Y. Fakhri, and D. Aboutajdine, "Impact of queue buffer size awareness on single and multi service real-time routing protocols for WSNs," *International Journal of Communication Networks and Information Security*, vol. 4, pp. 104–111, 2012.

[18] J. Sen, "A survey on wireless sensor network security," *International Journal of Communication Networks and Information Security*, vol. 1, pp. 55–78, 2009.

[19] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[20] S. Khan, K.-K. Loo, N. Mast, and T. Naeem, "SRPM: secure routing protocol for IEEE 802.11 infrastructure based wireless mesh networks," *Journal of Network and Systems Management*, vol. 18, no. 2, pp. 190–209, 2010.

[21] S. Khan, N. A. Alrajeh, and K.-K. Loo, "Secure route selection in wireless mesh networks," *Journal of Computer Networks*, vol. 56, no. 2, pp. 491–503, 2012.

[22] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 4, 2005.

[23] M. S. Siddiqui and S. H. Choong, "Security issues in wireless mesh networks," in *Proceedings of the International Conference on Multimedia and Ubiquitous Engineering (MUE '07)*, pp. 717–722, April 2007.

[24] S. Khan and K.-K. Loo, "Real-time cross-layer design for a large-scale flood detection and attack trace-back mechanism in IEEE 802.11 wireless mesh networks," *Network Security*, vol. 2009, no. 5, pp. 9–16, 2009.

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

[26] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of Sinkhole attacks in wireless sensor

networks," in *Algorithmic Aspects of Wireless Sensor Networks ALGOSENSORS*, vol. 4837 of *Lecture Notes in Computer Science*, pp. 150–161, Springer, 2008.

[27] H. Jadidoleslamy, "A hierarchical intrusion detection architecture for wireless sensor networks," *International Journal of Network Security & Its Applications*, vol. 3, no. 5, 2011.

[28] A. 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.

[29] A. 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.

[30] A. 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 ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet '05)*, pp. 16–23, Montreal, Canada, October 2005.

[31] 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.

[32] 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.

[33] M. S. Islam and S. A. Rahman, "Anomaly intrusion detection system in wireless sensor networks: security threats and existing approaches," *International Journal of Advanced Sciences and Technology*, vol. 36, pp. 1–8, 2011.

[34] 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.

[35] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," *Journal of High Speed Networks*, vol. 15, no. 1, pp. 33–51, 2006.

[36] C. 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.

[37] H. Deng, Q. A. Zeng, and D. P. Agrawal, "SVM-based intrusion detection system for wireless ad hoc networks," in *Proceedings of the 58th IEEE Vehicular Technology Conference (VTC '03)*, pp. 2147–2151, October 2003.

[38] Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," in *Proceedings of the 23th IEEE International Conference on Distributed Computing Systems*, pp. 478–487, May 2003.

[39] I. 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.

[40] M. 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.

[41] H. Sedjelmaci and M. Feham, "Novel hybrid intrusion detection system for clustered wireless sensor network," *International Journal of Network Security & Its Applications*, vol. 3, no. 4, 2011.

[42] R. Bhatnagar and U. Shankar, "The proposal of hybrid intrusion detection for defence of sync flood attack in wireless sensor network," *International Journal of Computer Science & Engineering Survey*, vol. 3, no. 2, pp. 31–38, 2012.

[43] K. 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 MultiConference of Engineers and Computer Scientists (IMECS '09)*, Hong Kong, 2009.

[44] K. 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.

[45] 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.

[46] S. Khan, K.-K. Loo, and Z. U. Din, "Cross layer design for routing and security in multi-hop wireless networks," *International Journal of Information Assurance and Security*, vol. 4, no. 2, pp. 170–173, 2009.

[47] D. E. Boubiche and A. Bilami, "Cross layer intrusion detection system for wireless sensor network," *International Journal of Network Security & Its Applications*, vol. 4, no. 2, 2012.

[48] M. Xiao, X. Wang, and G. Yang, "Cross-layer design for the security of wireless sensor networks," in *Proceedings of the 6th World Congress on Intelligent Control and Automation (WCICA '06)*, pp. 104–108, Dalian, China, June 2006.