Intrusion detection and security mechanisms for wireless sensor networks

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 747483, 3 pages
http://dx.doi.org/10.1155/2014/747483

Editorial

Intrusion Detection and Security Mechanisms for Wireless Sensor Networks

S. Khan,[1] Jaime Lloret,[2] and Jonathan Loo[3]

[1] *Institute of Information Technology, Kohat University of Science and Technology (KUST), Kohat City 26000, Pakistan*
[2] *Integrated Management Coastal Research Institute, Universidad Politecnica de Valencia, Camino de Vera, 46022 Valencia, Spain*
[3] *School of Science and Technology, Middlesex University, The Burroughs, London NW4 4BT, UK*

Correspondence should be addressed to S. Khan; skhan@kust.edu.pk

Received 2 February 2014; Accepted 2 February 2014; Published 4 March 2014

Wireless sensor networks are multihop, self-organizing, self-healing, and distributed in nature. One of their main features is their energy consumptions, so many efforts are focused on power saving techniques. Wireless sensor networks are gaining significant interest from academia and industry and the number of real deployments of wireless sensor networks (WSN) is increasing considerably in the last years. Their intrinsic characteristics make them very vulnerable to external intrusion. Thus, the security has become one of the main issues to study in WSNs. Their ad hoc network nature also increases their vulnerability and exposes sensor nodes to various kinds of security attacks. There is a clear need for new security techniques to guarantee the information transmitted through the WSN. Last research tendencies are focused on including security in the routing protocol, providing security for communication inside groups of nodes and when exchanging data between groups. One of the most efficient techniques to detect an intruder in the network is the use of traffic analysis for detecting anomalies and finding correlated events. Advanced security mechanisms and intrusion detection systems (IDSs) can play an important role in detecting and preventing security attacks in WSNs.

In this special issue, we have collected recent advances in intrusion detection and security mechanisms for WSNs. The papers have been peer reviewed and have been selected on the basis of their quality and relevance to the topic of this special issue.

There are many WSN applications; however, such networks are highly vulnerable to different security attacks such as altering, misusing, or misdirecting the data in transit. Keep these issues in mind. M. Usama and F. T. B. Muhaya present the paper "*Framework for secure wireless communication in wireless sensor networks*." The framework consists of few modules such as redundancy checker, message prioritization mechanism, malicious node verification, and malicious data verification. It is evaluated and validated using NS2 simulator. The experimental results show that the proposed secure framework can be used for malicious data or node detection.

There are many techniques which are used to design IDSs for WSNs. Artificial intelligence techniques are widely used for this purpose. In the paper "*Intrusion detection systems based on artificial intelligence techniques in wireless sensor networks*," a critical study on genetic algorithm, artificial immune, and artificial neural network (ANN) based IDSs techniques used in wireless sensor network (WSN) is presented. ANN concepts are helpful in many areas such as pattern recognition and intrusion detection. ANN based intrusion detection can be helpful to eliminate the shortcomings of rule based IDSs. However, ANN based IDSs can be more effective if properly trained with both normal and abnormal data sets.

In the paper titled "*Lightweight and scalable intrusion trace classification using interelement dependency models suitable for wireless sensor network environment*," a lightweight and scalable method for classification of network and detection of system intrusion attempts is presented. The authors claim better intrusion detection accuracy of the proposed system. The mechanism involves many actions such as

Naive Bayes Classifier, Naive Bayes with n-gram features, interdependency modeling, Support Vector Machines, and k-truncated suffix tree. Experiments are conducted with many data sets such as UNM and MIT LL 1998.

The authors of the paper "*Intrusion detection systems in wireless sensor networks: a review*" present a review of IDSs in WSN such as the following.

(i) *Signature based IDSs*—signature based IDSs are also known as rule based as they have predefined rules for different security attacks. These IDSs can only detect those security attacks whose signatures are present in the databases. The limitation of such detection mechanisms is that they cannot detect new or those attacks whose signatures are not present.

(ii) *Anomaly based IDSs*—anomaly based IDSs are intelligent and they do not have a support of predefined rules. These kinds of IDSs mostly use threshold value for classifying attacks.

(iii) *Hybrid IDSs*—hybrid IDSs use both mechanisms; that is, it is the combination of signature based approach and anomaly based approach. However, hybrids IDSs are not considered suitable for WSNs due to more complexity and heavyweight nature.

(iv) *Cross-layer IDSs*—as multihop wireless networks are vulnerable to multi-layer security attacks, and security mechanism for one layer cannot detect and respond to a security attack at another layer. Cross-layer IDSs are capable of detecting multilayer security attacks. However, as WSNs are resource constraint networks, that is why cross-layer IDSs are not considered suitable for such networks. The reason is that cross-layer IDSs exchange parameters across the protocol stake which may consume more power, memory, and processing.

Key management in a large cluster based sensor network with limited resources is a challenging task. Furthermore, an attacker can compromise the entire network security just controlling few nodes and injecting false data in an undetected manner. To protect WSNs from such impersonating attacks, G. Jeong et al. present a new dynamic key management framework particularly for large-scale clustered sensor networks in the paper "*Impersonating-resilient dynamic key management for large-scale wireless sensor networks*." In the framework, different keying mechanisms, respectively, secure in-cluster, intercluster, and individual communication by refreshing keys on demand, while adaptively handling node addition and capture. Experimental results show that the proposed framework provides higher security against impersonating attacks with less cost. The scheme can efficiently handle many scenarios such as node addition and eviction. The proposed solution also presents different keying mechanisms for different situations such as in-cluster, intercluster, and individual communication. It uses simple cluster-shared one-way key chain.

An eavesdropping attack with directional antennas in WSN is described in the paper "*On eavesdropping attacks in wireless sensor networks with directional antennas*." The proposed model analyzes the eavesdropping probability in both single-hop WSNs and multihop WSNs with omnidirectional antennas and directional antennas. It is demonstrated that to use directional antennas can significantly reduce the eavesdropping probability in both single-hop and multihop WSNs. Directional antennas provide more security due to the smaller region and the low number of hops in the route. The experimental results show that better security is dependent on the signal path loss factor, beam width, and node density. The paper has some interesting contributions such as

(i) eavesdropping modeling in WSNs with omnidirectional and directional antennas,

(ii) determination of exposure region to check whether an attacker can eavesdrop or not,

(iii) analysis of eavesdropping attacks in both single-hop networks and multihop networks with both omnidirectional antennas and directional antennas.

A game theoretic model for hidden-action attacks is proposed in the paper "*A game theoretic model for wireless sensor networks with hidden-action attacks*." This mechanism investigates the attack and detection problem by modeling it as pairwise simultaneous game and spatial structured game. In experimental results, different effects are analyzed such as

(i) action cost effect,

(ii) coaction effect,

(iii) stimulation effect,

(iv) punishment effect.

The authors are interested in extending this work in the future by adding some important features such as

(i) further enhancing the efficiency of the proposed mechanism to detect many other attacks,

(ii) estimating the cost of the game modeling in WSN,

(iii) considering more complex WSN models.

Security in cognitive wireless sensor networks (CWSN) is an important problem because these kinds of networks are used in critical and important applications. Moreover, the limited resources of WSN make the problem even more complex. The paper "*PUE attack detection in CWSN using collaboration and learning behavior*" is focused on primary user emulation (PUE) attack in CWSN. In PUE attack, a malicious node emulates the behavior of an incumbent node to use the radio spectrum for its own useless operation or stop the other nodes to access the spectrum. The authors claim that in most of the previously published works use traffic monitoring to train a behavior model of the network, while, in this work, other parameters such as power transmission to detect anomalies in CWSN are also considered. Many experiments are conducted to validate the behavior of the proposed system; it is observed that if the collaborative nodes are over 20% of the total, the PUE attack detection has satisfactory results, with 98% of attacks detected and a false negative rate near 0%.

The paper "*Evaluation, energy optimization, and spectrum analysis of an artificial noise technique to improve CWSN security*" focuses on physical layer security in CWSN. It discusses many aspects such as energy optimization, security evaluation, and spectrum analysis of artificial noise techniques to strengthen the physical layer security. The authors claim that these techniques introduce noise into the spectrum to hide real information. The important finding of this paper is an intelligent mechanism, in which the transmitter with the help of few supporting nodes is capable of generating noise in order to hide the data in transit. The noise is generated in such a way that only the attacker is affected, not the legitimate receiver.

External attacks can be detected easily as compared to internal attacks. In internal attack(s), the attacker is inside and most of the time is a legitimate member of the network. Detection of insider malicious node is a challenging task as it not only is a legitimate member of the network but also knows exactly what their neighbors or monitoring nodes know. Such insider malicious node can launch attacks secretly and carefully to avoid being detected and discarded from the network. In the paper titled "*Detection and prevention of selective forwarding-based denial-of-service attacks in WSNs*," a mechanism to detect insider malicious node capable of selective forwarding-based denial-of-service attack is proposed. The proposed scheme uses trust management approach to detect such malicious nodes and their victims. Furthermore, the authors designed two attacker-aware protocols to route victim nodes packets using alternate path to avoid attackers. The paper presents some interesting findings.

(i) Beta trust model and entropy trust model fail to detect selective forwarding attack.

(ii) The potential damage to the network due to such attacks is analyzed.

(iii) A source level trust management scheme is used to enhance the security features of beta and entropy models.

(iv) An avoidance strategy is presented to reroute the packets so as to avoid attackers.

(v) A preventive mechanism is also presented to prevent such attacks.

Adaptive ant based secure routing protocol to select two optimal paths keeping in view route security is proposed in the paper "*Secure ant-based routing protocol for wireless sensor network*." The proposed scheme has four important steps, that is, route discovery, route selection, route security, and data forwarding to destination. This mechanism is inspired from the real ants. Forward and backward ants are used for route request and route reply purpose. Furthermore, the forward ants collect and increment the reputation values along the path to ensure security. The scheme is compared with other candidate solutions such as LEACH and iACO protocols.

In the paper "*On lightweight intrusion detection: modeling and detecting intrusions dedicated to OLSR protocol*," a signature based IDS in cooperation with OLSR routing protocol is presented. Most of the existing IDSs monitor the ongoing traffic for attacks detection. Contrary to other solutions, the proposed system monitors and analyses logs for misuse detection.

S. Khan
Jaime Lloret
Jonathan Loo