Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2012, Article ID 582139, 6 pages
doi:10.1155/2012/582139

Research Article

A Congestion-Aware IDS Node Selection Method for Wireless Sensor Networks

Jaeun Choi,[1] Gisung Kim,[2] and Sehun Kim[3]

[1] *Department of Industrial & Systems Engineering, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-Gu, Daejeon 305-701, Republic of Korea*
[2] *KAIST Institute for Information Technology Convergence, 291 Daehak-ro, Yuseong-Gu, Daejeon 305-701, Republic of Korea*
[3] *Department of Industrial & Systems Engineering and Graduate School of Information Security, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-Gu, Daejeon 305-701, Republic of Korea*

Correspondence should be addressed to Jaeun Choi, juchoi@kaist.ac.kr

Received 10 February 2012; Revised 9 June 2012; Accepted 24 June 2012

Academic Editor: Sahin Albayrak

We propose an Intrusion Detection System (IDS) node selection method for Wireless Sensor Networks (WSNs). Due to the WSNs' distinctive tree structure, network congestion normally occurs in nodes that are located in the vicinity of a static base station. Moreover, in resource-constrained WSNs, network congestion could occur due to resource depletion attacks, such as Denial of Service (DoS) attacks. This congestion increases data loss and reduces the network's lifetime. In this paper, we propose an Intrusion Detection Systems (IDSs) construction method that considers this network congestion. Moreover, due to the limited battery life of sensor nodes, the proposed method is considered to be efficient in utilizing limited resources by selecting IDS nodes that enhance the network's lifetime and reduce the total energy consumption. The simulation results show that the proposed method enhances the network's lifetime and reduces the total energy consumption of the congested network.

1. Introduction

Wireless Sensor Networks (WSNs) have increasingly become one of the most widely used wireless networks over the past several years. Although WSNs belong to the class of general wireless networks, they have their own distinctive features. WSNs have tiny sensor nodes and simple devices with restricted transmission power and limited energy. Due to the limited battery of sensor nodes, sensor networks are more vulnerable to resource depletion attacks, one of the major problems in wireless sensor networks. Thus, security solutions for wireless sensor networks have to be designed that consider the battery consumption and the limited battery life of sensor nodes [1].

An Intrusion Detection System (IDS) for wired networks is widely employed for security purposes to detect illegal intrusions that are considered to be unauthorized or abnormal [2]. However, most intrusion detection techniques are not suitable for wireless networks since they utilize open media and collaborative algorithms and lack centralized monitoring and management points [3, 4]. Therefore, an *ad hoc* intrusion detection architecture is needed for wireless networks. Especially in WSNs, besides the problems mentioned above, the IDS has to solve the problems imposed by the limited battery life and computational power of sensors [4].

To secure mobile computing applications, an anomaly intrusion detection architecture (AD) is proposed, in which every node in the wireless network participates in intrusion detection [3]. The AD scheme provides intrusion detection facilities into wireless nodes, and they are called IDS nodes. As an IDS node overhears and analyzes all packets within its monitoring range, the IDS node consumes more resources than non-IDS nodes [2]. In terms of limited network resources, the AD scheme, which has many IDS nodes in the network, is inefficient. Moreover, the major problem with this approach is that one node usually receives the same monitoring services from all neighbor IDS nodes. Therefore, an efficient IDS node selection method is needed in order to utilizing the limited wireless network resources.

For selecting IDS nodes in wireless networks, a distributed IDS node selection scheme (DIDS) is proposed for wireless *ad hoc* networks that allocates intrusion detection tasks to nodes with high connectivity [5]. The advantages of the DIDS scheme are that the overall packet-monitoring task is limited to a small number of IDS nodes. However, the lifetime of the whole network decreases since the monitoring load becomes easily concentrated at the IDS nodes that have high connectivity. Accordingly, IDS nodes suffer from battery depletion. In particular, packet congestion of IDS nodes could frequently occur under heavy network load situations because the links, which are connected to IDS nodes, carry many data packets. This congestion can reduce the network's lifetime due to excessive monitoring tasks.

To enhance network lifetime, a lifetime-enhancing monitoring node Selection (LES) scheme is proposed [2]. The LES scheme selects nodes that have a maximum amount of battery remaining as IDS nodes among the neighboring nodes. Compared to the DIDS scheme, the LES scheme enhances the network's lifetime. However, the LES scheme usually requires many IDS nodes in the network because every node that has more energy than the neighboring nodes is selected as an IDS node. Due to the energy consumption by too many IDS nodes, the total energy consumption in the LES scheme is quite high. Moreover, since LES and DIDS do not consider the network's traffic status in selecting IDS nodes, the nodes suffering from packet congestion could be selected as IDS nodes. This may cause a short lifetime for the whole network and high energy consumption.

In this paper, we propose a congestion-aware IDS node selection method for WSNs. Our method differs from the previous methods by considering network congestion. Due to their inherent limitations, WSNs are especially sensitive to network congestion. The applications of WSNs require the sensor nodes to periodically collect and transmit data towards a base station. Such tree structure of WSNs can cause congestion while data loss would normally occur at the nodes located in the vicinity of a static base station. Congestion at these nodes occurs due to the fact that at any given point of time a base station can only communicate with one, or a limited number, of the sensor nodes [6]. In resource-constrained WSNs, network congestion could also occur by resource depletion attacks, such as Denial of Service (DoS) attacks.

When choosing IDS nodes, it is important to consider network congestion. The packets are buffered in the queue of a monitoring node for IDS inspection. When congestion occurs in the buffer of an IDS node due to high packet arrival rates, the IDS node cannot afford to monitor all of the arrival packets and buffer overflow occurs. This congestion may cause a decline in the detection rate and high energy consumption of IDS due to excessive monitoring tasks. In this paper, we propose an IDS node selection method that considers both the remaining battery life of nodes and network traffic. This method utilizes queuing theory in order to reduce the possibility of packet congestion in the buffer of an IDS node. The simulation results show that our method can enhance the network's lifetime and reduce the energy consumption of the whole network.

This paper is organized as follows. Section 2 reviews related work. Section 3 describes the proposed algorithm in detail. Performance measurement is discussed in Section 4, and in Section 5, the algorithm is evaluated. The study concludes in Section 6 with a summary of the results.

2. Related Work

An IDS is widely used to detect intrusions in wired and wireless networks. Unlike wired networks, wireless networks communicate with each other using an open medium and face resource constraints of nodes. As such, these characteristics must be considered in the IDS design. There have been some studies about intrusion detection architectures for wireless networks.

As mentioned earlier, an AD scheme serving as an IDS for all nodes was suggested to ensure wireless network security [3]. This method is inefficient because all nodes are required to participate in detecting intrusions. The DIDS [5] and LES [2] schemes were introduced to overcome such inefficiency through IDS selection. Another IDS selection method was proposed to apply LES while excluding suspicious nodes [7]. Although DIDS and LES are able to enhance efficiency by eliminating redundancy, these schemes entail other problems. Moreover, methods that enable efficient allocation of IDS are usually targeted in *ad hoc* networks. The WSN examined in this paper possesses different characteristics from those of an *ad hoc* network and thus requires a different approach in IDS selection.

First, a WSN consists of a base station and sensor nodes, whereas an *ad hoc* network is comprised of nodes alone. Sensor nodes transmit collected data and information to the central base station and the base station is then able to assess the state of the network. Because an *ad hoc* network lacks a central coordinator, the IDS selection proceeds based on distributed information at each node. However, in the case of WSNs, a centralized solution is possible using network information at the base station. By providing a centralized solution to IDS selection, the overall network efficiency can be enhanced since the entire network status is considered instead of distributed information. An earlier study proposed a similar method to DIDS, selecting high-connectivity nodes as an IDS for WSNs [8]. However, this method provided the form of a distributed solution. In this paper, we present a centralized solution to IDS selection while taking into account the characteristics of WSNs.

Another point to consider for WSNs is the limited capacity of sensor batteries. Malicious attacks may exploit this characteristic by exhausting batteries after causing congestion in sensor nodes with heavy traffic [9]. Given the structural characteristic of WSNs, traffic is likely to be concentrated at the base station, thus placing surrounding nodes at risk of congestion. In WSNs, congestion should be avoided as batteries will be rapidly depleted. The IDS selection method suggested in this paper accounts for congestion, which has not been considered in other methods.

3. Algorithm

In this section, we propose a two-stage IDS node selection method that consists of an IDS node selection stage and a normal node assignment stage. In the IDS node selection stage, IDS nodes were selected in the WSN by using an optimization method. In the normal node assignment stage, a set of normal nodes was assigned to each IDS node in order to avoid redundant checks.

3.1. Stage (1) Selecting IDS Nodes. The main interest here is packet congestion avoidance in IDS nodes. Packet congestion occurs when a node handles so many packets at once that its quality of service deteriorates. This congestion can cause queuing delay and packet loss.

IDS nodes should be selected among nodes that do not have congestion. In order to define noncongested nodes, let us first consider a network where, if a node is selected as an IDS node, the node operates its IDS function and monitors all of the packets that come into the node. In noncongested IDS nodes, no packet should wait in line in the buffer of IDS nodes for longer than a given time limit [10]. This constraint is as follows:

$$P[\text{packet}'\text{s waiting time in IDS node } j \le \tau] \ge \alpha, \quad \forall j, \tag{1}$$

where the variables τ and α are predefined time and probability. Constraint (1) makes the total time spent by a packet in the IDS node j shorter than or equal to τ with a probability of at least α. If constraint (1) is satisfied in a node, the node is regarded as a noncongested IDS node.

To express constraint (1) as a numerical formula, we define f_{ij} as the average packet arrival rate from node i to j. Then, the total arrival rate to node j can be expressed as

$$F_j = \sum_{i \in N} f_{ij} a_{ij}, \tag{2}$$

where set N is the set of all nodes in the network and binary value a_{ij} is one if node j is in the transmission range of node i, and zero otherwise Figure 1.

From queuing theory [10], it is easy to conclude that if the total arrival rate to node j, F_j, is less than or equal to

$$D_j = \mu_j + \frac{1}{\tau} \ln(1 - \alpha), \tag{3}$$

then the time delay of a packet in node j is shorter than or equal to a τ with a probability of at least $\alpha(> 0)$, where τ is a predetermined time interval and μ_j is the monitoring service rate in node j. Therefore, a node j, such that $F_j \le D_j$, can be regarded as a noncongested node. Our IDS node selection method suggests choosing IDS nodes from

$$S = \left\{ j \mid F_j \le D_j, j \in N \right\}, \tag{4}$$

which is the set of noncongested nodes.

IDS nodes are selected in set S by using an optimization method. The IDS nodes should be selected so that the overall cost of monitoring tasks for all IDS nodes is minimized while satisfying a coverage constraint. In order to monitor all of the nodes in the network, every node should be in the monitoring coverage of at least one IDS node. In order to utilize wireless resources efficiently, we want to minimize the overall cost of monitoring tasks by the IDS nodes. Our proposed formulation is as follows:

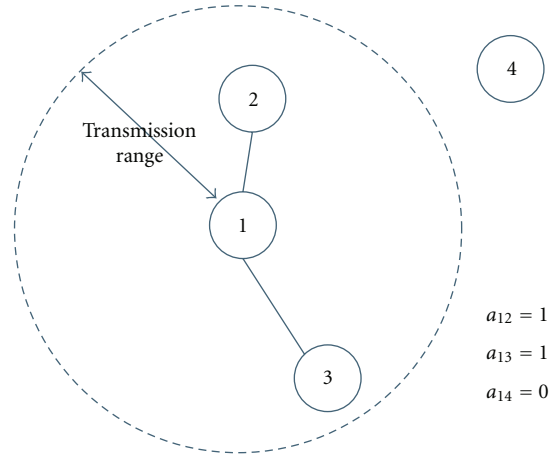

Figure 1: Definition of a_{ij}.

$$\min \sum_{j \in S} c_j x_j, \tag{5}$$

subject to

$$\sum_{j \in S} a_{ij} x_j \ge 1, \quad i \in N, \tag{6}$$

$$x_j \in \{0, 1\}, \quad j \in S, \tag{7}$$

where c_j is the cost of node j and x_j is the binary variable, which is one if node j is an IDS node, and zero otherwise. In our proposed formulation, IDS nodes are selected in set S. Therefore, we could reduce the possibility of packet congestion in IDS nodes. Moreover, the objective function (5) minimizes the total cost of the entire network. If we define c_j as 1, the objective function minimizes the number of IDS nodes under the constraints, resulting in a reduction of the total energy consumption. If we define c_j as the negative value of node j's remaining battery, we can enhance the network's lifetime simultaneously with a reduction in the total energy consumption. In this case, our formulation prevents a node with low battery from being selected as an IDS by maximizing the sum of all the IDS node's remaining battery. Therefore, we are able to enhance the network's lifetime. In objective function (5), by adjusting c_j, we can acquire a trade-off solution between the network's lifetime and the total energy consumption.

Constraint (6) states that every node should be located in the transmission range of at least one IDS node. Hence, this constraint satisfies the requirement that all nodes are monitored by IDS.

Define the set M as the set of IDS nodes,
and the set N as the set of all nodes
$M = \{i \mid x_i = 1\} \quad N = \{1, \ldots, n\}$
step 1. Node k, which has maximum remaining battery (b_i) in the set M, monitors its neighbor node set N_c
$k = \arg_i \max b_1.$
$N_c = \{j \mid a_{kj} = 1, \quad j \in N\}$
step 2. Remove the set N_c from the set N, and remove the node k from the set M
$N = N–N_c, \quad M = M–k$
step 3. If the set N is empty, then stop. Otherwise, go to the step 1.
if $N = \emptyset$ *then STOP else Goto step* 1

Algorithm 1: The assignment algorithm.

3.2. Stage (2) Assigning Nodes to IDS Nodes. By using the proposed formula, IDS nodes were selected among all of the nodes in the network. Next, a set of normal nodes are assigned to each of the IDS nodes without redundant monitoring. In previous related studies, the IDS node monitored all the neighboring nodes. This resulted in the normal node being monitored by all the neighboring IDS nodes. To prevent this redundant check, we propose an assignment algorithm that enables the normal node to be monitored by one IDS node. In our algorithm, an IDS node with maximum battery life monitors all of its neighbors first. Next, an IDS node with the second-highest battery life monitors its neighbors, except for the neighboring nodes of the maximum battery IDS node. The assignment algorithm is operated until all normal nodes are allocated to the IDS nodes. For this algorithm, the less battery life the IDS nodes have, the fewer nodes they monitor. Therefore, the proposed algorithm is able to enhance the network's lifetime. The assignment algorithm is shown in Algorithm 1.

4. Performance Measure

A normal node uses its energy for transmission and reception. Additionally, the IDS node overhears packets within the monitoring range and analyzes them to detect intrusions. The energy consumed by a monitoring node is calculated as

$$E = (m^t s^t + b^t) + (m^r s^r + b^r) + (m^o s^o + b^o) + (m^m s^m + b^m), \tag{8}$$

where s^t, s^r, s^o, and s^m, respectively, represent the packet sizes for transmission, receiving, overhearing, and monitoring operations. Factors m and b are variables and fixed energy costs for each operation [11]. We will show numerical simulations by using (8).

We consider the network's lifetime and the networks' total energy consumption as meaningful performance measures. The network's lifetime is defined as the duration of time until the first node runs out of battery. If a single node runs out of battery, this battery depletion could separate the network into unconnected subnetworks making further communication impossible between unconnected networks [2]. Therefore, enhancing the network's lifetime is important for the stability of the network. As wireless sensor networks have constraints on limited energy, the total energy consumption should be reduced while providing a required level of intrusion detection in networks. Hence, total energy consumption was selected as a performance measure for utilizing limited resources efficiently. In this paper, the sum of the remaining battery life was defined as the total remaining battery life in the network when the first node exhausts its battery. From this measure, we can know the total energy consumption of the whole network. By showing the numerical results of these measures, we will know how efficiently the proposed algorithm can utilize network resources.

5. Simulation Results

In this section, the performance of the proposed algorithm is analyzed by using computer simulation on Matlab. The DIDS and LES schemes that were mentioned before were compared to the proposed algorithm. In this simulation, 20 nodes were deployed in a wireless sensor network. A certain amount of packets destined for random nodes were generated with a packet size of 512 bytes. Furthermore, we assumed that all nodes had the same initial battery power. The amount of battery energy consumed by each node was calculated using (8) of the previous section. In this simulation, in order to consider the network's lifetime and the total energy consumed simultaneously, c_j was set as the negative value of node j's remaining battery. One hundred iterations were run to achieve an average performance.

The performance measures were evaluated in the congested network. Network congestion was generated when a link or node carried too many data packets. Figure 2 shows the average network's lifetime in congested systems. In Figure 2, each broken line represents the average network lifetime and the horizontal axis represents the average size of the packets that each node sends. Even if traffic becomes heavier, the network's lifetime under the proposed scheme is

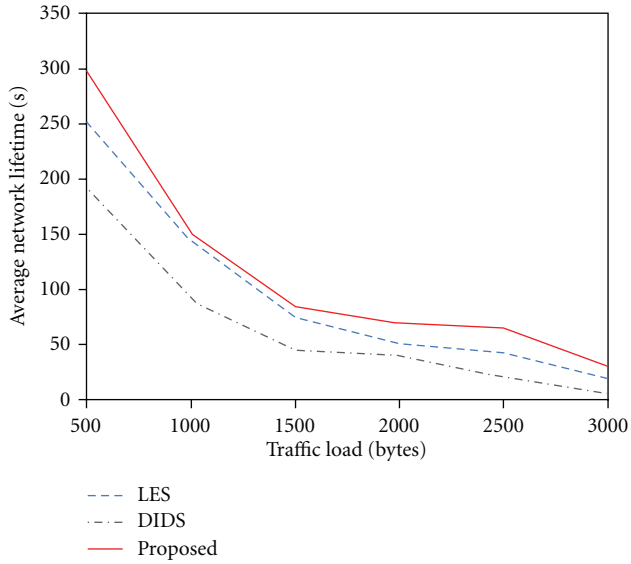

Figure 2: Network's lifetime in congested network.

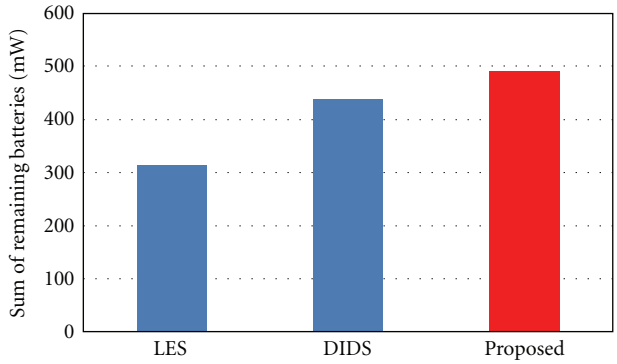

Figure 3: Sum of remaining batteries in congested network.

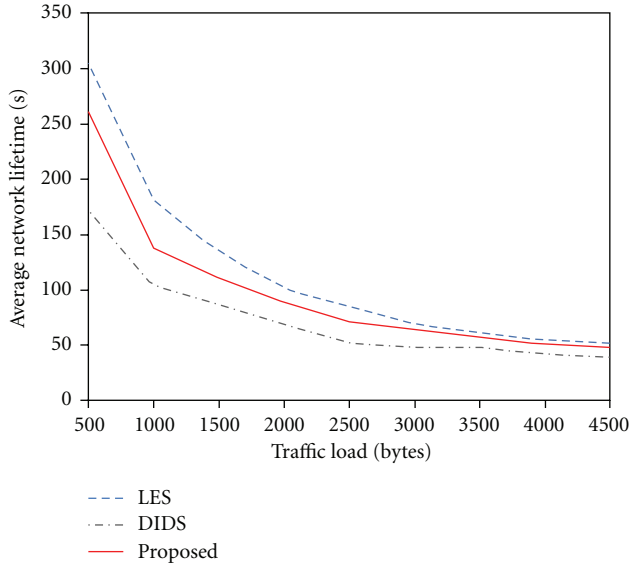

Figure 4: Network's lifetime in normal network.

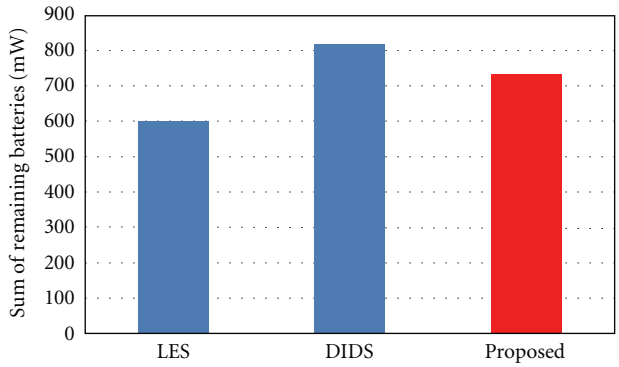

Figure 5: Sum of remaining batteries in normal network.

longer than or similar to that under LES. Figure 3 shows the sum of remaining batteries in a congested network and each bar represents the sum of remaining batteries. The sum of the remaining batteries in the proposed scheme was found to be the largest among the three schemes. Since our algorithm differs from other methods by preventing the congestion of packets in the IDS nodes, the proposed scheme outperforms the other existing schemes in a congested network.

Next, performance measures were evaluated in a normal network environment that does not suffer from traffic congestion. In Figure 4, the network lifetimes under different algorithms are compared. Unlike the other methods, the proposed method was found to outperform DIDS in terms of network lifetime. In Figure 5, the sum of the remaining batteries of the proposed method is shown to be always higher than that of LES. Our proposed method minimizes the number of IDS nodes under the constraints while preventing nodes with low battery life from being selected as IDS nodes. Moreover, our allocation algorithm enhances the network's lifetime by removing redundant monitoring. Therefore, we can acquire trade-off results for the network's lifetime and total energy consumption.

6. Conclusion

In this paper, we proposed an IDS selection method that aims at enhancing the network's lifetime and reducing the total energy consumption, while preventing congestion due to monitoring. In congested situations, our proposed method performed better than the other existing methods. Moreover, in a normal network, our proposed method allows a longer lifetime than DIDS. Our method also shows that the battery energy consumed by the entire network is less than under LES.

Our future research will focus on improving the energy efficiency in a normal network. Furthermore, to reduce calculation time, heuristic algorithms will be required.

Acknowledgment

This paper was supported by the MKE (The Ministry of Knowledge Economy), Republic of Korea, under the CYBER

SECURITY RESEARCH CENTER supervised by the NIPA (National IT Industry Promotion Agency), NIPA-C1000-1101-0001.

References

[1] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '05)*, pp. 253–259, Montreal, Canada, August 2005.

[2] H. Kim, D. Kim, and S. Kim, "Lifetime-enhancing selection of monitoring nodes for intrusion detection in mobile Ad Hoc networks," *AEU—International Journal of Electronics and Communications*, vol. 60, no. 3, pp. 248–250, 2006.

[3] Y. Zhang, W. Lee, and Y. A. Huang, "Intrusion detection techniques for mobile wireless networks," *Wireless Networks*, vol. 9, no. 5, pp. 545–556, 2003.

[4] L. Mostarda and A. Navarra, "Distributed intrusion detection systems for enhancing security in mobile wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 4, no. 2, pp. 83–109, 2008.

[5] O. Kachirski and R. Guha, "Effective intrusion detection using multiple sensors in wireless Ad Hoc networks," in *Proceeding of the 36th Annual Hawaii International Conference on System Sciences (HICSS '03)*, pp. 57–64, Big Island, Hawaii, USA, January 2003.

[6] M. I. Khan, W. N. Gansterer, and G. Haring, "Congestion avoidance and energy efficient Routing protocol for wireless sensor networks with a mobile sink," *Journal of Networks*, vol. 2, no. 6, pp. 42–49, 2007.

[7] M. K. Rafsanjani, A. A. Khavasi, and A. Movaghar, "An efficient method for identifying IDS agent nodes by discovering compromised nodes in MANET," in *Proceedings of the International Conference on Computer and Electrical Engineering (ICCEE '09)*, pp. 625–629, Dubai, UAE, December 2009.

[8] T. H. Hai and E. N. Huh, "Minimizing the intrusion detection modules in wireless sensor networks," in *Proceedings of the International Conference on Computational Sciences and its Applications (ICCSA '08)*, pp. 184–189, Hong Kong, Hong Kong, July 2008.

[9] M. Khanafer, M. Guennoun, and H. T. Mouftah, "Intrusion detection in WSN-based intelligent transportation systems," in *Proceedings of the 1st ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, pp. 117–122, Miami, Fla, USA, 2011.

[10] V. Marianov and M. Ríos, "A probabilistic quality of service constraint for a location model of switches in ATM communications networks," *Annals of Operations Research*, vol. 96, no. 1–4, pp. 237–243, 2000.

[11] L. M. Feeney and M. Nilsson, "Investigating the energy consumption of a wireless network interface in an Ad Hoc networking environment," in *Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '01)*, pp. 1548–1557, Anchorage, Alaska, USA, April 2001.