A New Energy Prediction Approach for Intrusion Detection in Cluster-Based Wireless Sensor Networks

Wen Shen[1,2], Guangjie Han[1,2], Lei Shu[3], Joel J.P.C Rodrigues[4],
and Naveen Chilamkurti[5]

[1] Department of Information & Communication Systems, Hohai University, China
[2] Changzhou Key Laboratory of Sensor Networks and Environmental Sensing, China
[3] Department of Multimedia Engineering, Osaka University, Japan
[4] Instituto de Telecomunicações, University of Beira Interior, Portugal
[5] Dept. of Computer Science and Computer Engineering, La Trobe University, Australia
{hanguangjie,shen.wen1986}@gmail.com, lei.shu@live.ie,
joeljr@ieee.org, n.chilamkurti@latrobe.edu.au

Abstract. Wireless Sensor Networks (WSNs) require an efficient intrusion detection scheme to identify malicious attackers. Traditional detection schemes are not well suited for WSNs due to their higher false detection rate. In this paper, we propose a novel intrusion detection scheme based on the energy prediction in cluster-based WSNs (EPIDS). The main contribution of EPIDS is to detect attackers by comparing the energy consumptions of sensor nodes. The sensor nodes with abnormal energy consumptions are identified as malicious attackers. Furthermore, EPIDS is designed to distinguish the types of denial of service (DoS) attack according to the energy consumption rate of the malicious nodes. The primary simulation experiments prove that EPIDS can detect and recognize malicious attacks effectively.

Keywords: Wireless Sensor Networks, Intrusion Detection, Energy Prediction, DoS, Attacks Recognition.

1 Introduction

Many WSNs are organized into clusters to raise their security [1]. However the broadcast nature of wireless communication causes WSNs vulnerable to various malicious attacks. More specifically these networks are vulnerable to DoS attacks due to the use of the clustering scheme in real-world scenarios. Cluster head nodes are elected to manage local clusters, which are ideal targets for adversaries to compromise. If one single node is captured by adversaries and turned into malicious head, an entire local cluster would be affected by DoS attacks. This highlights the fact that the cluster-based WSNs require an efficient intrusion detection scheme to detect DoS attacks such as selective forwarding, wormhole attack and Sybil attack etc.

There are only a few intrusion detection methods [2, 3] proposed in the research literatures which are cluster-based in WSNs. The existing intrusion detection methods can be briefly classified into two categories: signature based detection and anomaly based detection [4]. Both of these two categories focus on identifying the behaviors of

Joel J.P.C. Rodrigues et al.: (Eds.): GreeNets 2011, LNICST 51, pp. 1–12, 2012.

malicious nodes and consume large quantity of energy in monitoring suspicious nodes. The disadvantage of traditional intrusion detection schemes is that the network lifecycle may become shorter as the schemes process large quantity of data and transmit it frequently. Moreover the networks suffer a high false detection rate as their detection schemes are deceived by DoS attacks. Hence, traditional intrusion detection schemes are not suitable for cluster-based WSNs, and it is critical to develop an effective security mechanism for WSNs to defend DoS attacks.

In this paper, we adopt EPIDS in a cluster-based WSN. Sensor nodes can be managed locally by cluster heads. Rotating cluster heads makes it possible to elect malicious nodes as cluster heads. Adversaries can compromise any node in the network and launch DoS attacks such as selective forwarding, hello flood, wormhole, sink hole and Sybil attack. As malicious nodes require abnormal energy to launch an attack, we focus on malicious nodes' energy consumption rate in order to discover the compromised nodes.

The two notable features of our scheme are listed as follows:

- In contrary with the traditional intrusion detection methods which only detect malicious attacks based on behavior or interactions between nodes within a period of time. We believe our energy consumption rate approach in this paper is novel and has many advantages. An energy prediction method is introduced to predict all the nodes' energy consumption rate in base station and detect some energy sensitive attacks which require abnormal energy.
- Furthermore, EPIDS distinguishes various malicious attacks according to the energy consumption rate. Energy thresholds are set to classify the malicious attacks, so that we can be aware of the types of attacks.

To our best knowledge, the concept of energy prediction in intrusion detection area has never been discussed in any previous research works. These two specific features mentioned above collectively make EPIDS a new, lightweight and efficient solution that can detect various attacks applied in any cluster-based WSNs.

The rest of this paper is organized as follows: section 2 introduces related work of intrusion detection schemes in WSNs. Section 3 presents an energy prediction model of sensor nodes. Section 4 introduces the energy prediction-based intrusion detection scheme in cluster-based WSNs. In Section 5 we discuss simulation results and evaluations of our scheme.

2 Related Work

There are few existing studies in detecting and preventing DoS attacks in WSNs. Related papers [2-4] always focus on the misbehaviors of sensor nodes. The security schemes allocate considerable resources to monitor the behaviors of all the sensor nodes. After the detection of malicious nodes, most schemes establish a blacklist to isolate malicious nodes. However, none of them adopts the energy character in detecting malicious nodes.

In [4] authors proposed a technique known as Spontaneous Watchdogs. This technique use both local and global agents to watch over the communications.

For hierarchal sensor networks, global agents are activated in every cluster head. For every packet circulating in the network, global agents with the Spontaneous Watchdogs technique are able to receive both the packet and the relayed packet by the next-hop. If malicious nodes modified or selective forwarded packets, the global agents will detect the attack by Spontaneous Watchdogs.

In [5] authors proposed an insider attacker detection scheme. The scheme explores the spatial correlation existent among the networking behavior of sensors in close proximity. The author considers multiple attributes simultaneously in node behavior evaluation, with no requirement on a prior knowledge about normal or malicious sensor activities. Moreover, the scheme employs original measurements from sensors and can be employed to monitor many aspects of sensor networking behavior.

In [6] authors proposed an analytical model for intrusion detection. The authors derive the detection probability by considering two sensing models: single-sensing detection and multiple-sensing detection. In addition, the paper discusses the network connectivity and broadcast coverage, which are necessary conditions to ensure the corresponding detection probability in a WSN.

In [7] authors proposed an energy-efficient intrusion detection system for wireless sensor network based on MUSK (**M**uhammad **U**sman and **S**urraya **K**hanum) agent. The MUSK agent is installed on each node that continuously monitors intrusion. The authors assume that MUSK agents are resilient against malicious nodes that try to steal or modify information carried by the agent. However, this assumption may not be realistic in many applications.

In [8] authors proposed a group-based intrusion detection system in WSNs. The group-based intrusion detection system first divides the sensor nodes into a number of groups using δ-grouping algorithm such that the nodes in a group are physically close to each other. This feature makes it easier to detect outlier nodes and the intrusion detection results become more precise then the scheme adopts the Mahalanobis distance measurement and the OGK estimators in the intrusion detection algorithm to ensure a high breakdown point even with some missing data. However, the author assumes that there is no intense or unexpected varieties of sensed data at the grouping phase of the intrusion detection algorithm. This assumption makes the algorithm not perfect.

In [9] authors provided an energy-efficient and secure system eHIP for cluster-based WSN. The eHIP system consists of Authentication-based Intrusion Prevention (AIP) subsystem and Collaboration-based Intrusion Detection (CID) subsystem. However, collaborative monitoring of each sensor nodes would cost abundant resources of the network and low the efficiency of communication between sensor nodes.

Sensor nodes with limited resources cannot constantly monitor other nodes behavior, and report any unusual behavior to their base station or neighbor nodes. Also a compromised node can return a false alarm, which is difficult to detect. Since the nature of wireless channels implies that packet forwarding is unstable, data packets would be lost during the transmissions. Therefore, security schemes which focus on the behaviors of sensor nodes could not detect the *selective forwarding* attack efficiently. For sensor node equipped with batteries, they can not be recharged after deployment, EPIDS could analyze the energy consumption of sensor nodes and is not affected by the interference of packet loss. Our proposed approach minimizes the security control messages and eliminates the need of updating monitor reports.

3 Energy Prediction Model

We believe that malicious nodes have to use additional energy to launch DoS attacks. Therefore, we preliminarily focus on an energy prediction method to detect malicious nodes. In this paper, Markov chains model is adopted to periodically predict energy consumption of sensor nodes. The difference between the predicted and the real energy consumption of sensor nodes can be used to detect malicious nodes.

3.1 Energy Dissipation

The energy dissipation in sensor nodes depends on the energy consumption in different working states and the time they operate in each state. The sensor nodes have five operation states: 1) *Sleeping* state: a sensor node operates in *sleeping* state does not interact with other nodes. Therefore, there is no need to evaluate the trust of the sleeping node. The energy dissipation of the sleeping node in the round time is E_{sleep}; 2) *Sensing* state: in the sensor operation, sensor nodes are responsible to sensing physical parameters, such as temperature, atmospheric pressure etc.; 3) *Calculating* state: sensor nodes process the received data; 4) *Transmitting* state: sensor nodes transmit data packets between the clusters and the base station; 5) *Receiving* state: sensor nodes receive data packets.

It is believed that the energy dissipation mainly focuses on the last four states. Therefore, each sensor node can be modeled by a Markov chain [10] with the last four states.

3.2 Operation State Transition Model

As shown in Fig.1, the operation states of any sensor node shift when the node sends and receives packets, calculates data and senses information. Furthermore, the time-step is the minimum time unit of the four operation states. Each state covers several time-steps. In one time-step, state i shifts to state j with a probability of P_{ij}, for $i, j = 1, 2, 3, 4$.

In a series of *n* time-steps, the operation states of a sensor node can be denoted as $X = \{X_0, X_{1,} ..., X_n\}$. $P_{ij}^{(n)}$ represents the probability of transition from state i to state j in n time-steps. Therefore, the *n*-stage transition probabilities can be defined as:

$$P_{ij}^{(n)} = P\{X_n = j \mid X_1 = i\} \tag{3.1}$$

$P_{ij}^{(n)}$ can be calculated by the *Chapman-kolmogorov* equations*:*

$$P_{ij}^{(n)} = \sum_{k=0}^{n} P_{ik}^{(r)} P_{kj}^{(n-r)} \quad 0 < r < n \tag{3.2}$$

If a cluster head knows $P_{ij}^{(n)}$ for its sensor nodes as well as the initial states X_0 of sensor nodes, it is possible to predict the energy consumption information of all sensor nodes in the cluster. The prediction process is shown as follows: Firstly, when the sensor node is current in state i, the cluster head counts the number of time-steps the node will stay in state j, $\sum_{t=1}^{T} P_{ij}^{(t)}$ Secondly, the cluster head calculates the amount of energy dissipation in the next T time-setps, E^T :

$$E^T = \sum_{j=1}^{4} (\sum_{t=1}^{T} P_{ij}^{(t)}) * E_j \tag{3.3}$$

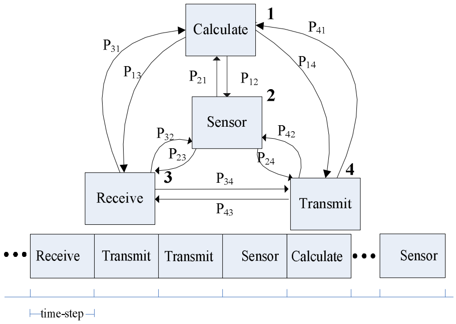

Fig. 1. The shift of operation states

Let E_j be the amount of energy dissipated in state j for one time-step. Finally, the cluster head node calculates the energy dissipation rate (ΔE) of the sensor node for the next T time-steps. The cluster head node can maintain estimations for the dissipated energy in each node by decreasing the value ΔE periodically for the amount of the remaining energy from each node. Given the energy dissipation prediction, cluster heads send the prediction results to the base station where trust information is stored.

4 Energy Prediction Based Intrusion Detection Scheme

According to the energy prediction method, EPIDS first compares the energy prediction results with the actual energy consumption at the node. Then the scheme searches nodes which spent significantly abnormal energy than other remaining nodes. The nodes with abnormal energy consumption are regarded to be malicious. Finally our scheme classifies the types of DoS attacks launched by malicious nodes.

4.1 Intrusion Detection Scheduling Algorithm

In the beginning of a round, sink node S predicts the energy consumption of each sensor node and keeps the prediction result. Then, at the end of each round, sink node is responsible for gathering energy residual of sensor nodes. Sink node broadcast an energy gathering message. On the responses to the energy gathering messages, the sensor nodes check their energy residual E_r and reply sink node with new value of E_r. If EPIDS scheme detects abnormal energy consumed at a node i, EPIDS will regard the node i as malicious and record the node's ID in a blacklist v. Sensor nodes in the blacklist will be segregated from the sensor network by removing it from the route table.

Table 1. The notations used in the intrusion detection algorithm

Notation	Meaning
S	Sink node
i	A sensor node
$Round$	the number of current round
E_p	the energy prediction result
E_r	the energy residual
R_{ID}	the set of nodes alive in this round
$Reply_{ID}$	the ID of node who reply this message
T	Timestamp
U	the set of nodes in the write list
v	the set of nodes in the black list

Table 2. Intrusion detection scheduling algorithm

```
If (Not clustering) And (receive <"clustering", $S$, $round_i$, $u$ >)
Then
  Broadcast <$S : u$, "Energy gathering", $round$, $R_{ID}$, $T$>
  If ($node_i = alive$) and ( $i \in u$ ) Then
    $E_r(i)=E(i)$;
    $Round=round_i$;
    Broadcast < $i$——> $S$ : $E_r(i)$, $round$, $Reply_{ID}$, $T$ >
  Else if ($node_i = alive$) and ( $i \in v$ ) Then
    $node_i$ is regarded as malicious and isolated;
  End if
  Else if (Not clustering) And (receive < $i$——> $S$ : $Er(i)$, $round$, $Reply_{ID}$, $T$ >) Then
    Store <$S$ :$i$, $E_r(i)$, $E_p(i)$, $round_i$, $Reply_{ID}$,>;
  End if
End if
```

4.2 Intrusion Detection Algorithm

The energy comparison between the energy prediction result and the energy consumption is the key to detect malicious nodes. Sink node records a set of energy residuals at the end of last round $\{r_1, r_2, r_3, ..., r_{m\times n}\}$. Then in the next round, sink node makes a prediction of energy consumption of sensor nodes, denoted as $\{p_1, p_2, p_3, ..., p_{m\times n}\}$. After receiving the residual energy $\{r_1', r_2', r_3', ..., r_{m\times n}'\}$ from all sensor nodes, the actual energy consumption is $\{r_1 - r_1', r_2 - r_2', r_3 - r_3', ..., r_{m\times n} - r_{m\times n}'\}$ calculated at the sink node. Therefore, the energy comparison of each node forms the set $\{p_1 - (r_1 - r_1'), p_2 - (r_2 - r_2'), p_3 - (r_3 - r_3'), ..., p_{m\times n} - (r_{m\times n} - r_{m\times n}')\}$. If $|p_i - (r_i - r_i')| > T_{reshold}$, $i \in [1, m\times n]$, then node *i* would be regarded as malicious.

4.3 Malicious Nodes Classification Algorithm

After the intrusion detection, the network identifies the types of DoS attacks launched by these malicious nodes.

Let E_c denote the energy comparison results:

$$E_c = E_p - E_r$$

E_p and E_r represent the energy prediction result and the energy real consumption of a sensor node *i*. *k* is the size of the data packet.

The possible five DoS attacks can be divided into two sets, $Attack_1$ and $Attack_2$, where $Attack_1 = \{\mathrm{A}_1\}$ and $Attack_2 = \{\mathrm{A}_2, \mathrm{A}_3, \mathrm{A}_4, \mathrm{A}_5\}$. A_1 represents a *selective forwarding* attack; A_2, A_3, A_4, and A_5 represent *Hello flood* attack, *Sybil attack*, *Wormhole attack* and *Sinkhole attack,* respectively. $Attack_1$ is a set that include DoS attacks that energy consumptions are lower than prediction results, and $Attack_2$ is a set that includes DoS attacks that energy consumptions are lower than prediction results. To classify these five DoS attacks, our scheme sets four domains $D = \{\mathrm{D}_1, \mathrm{D}_2, \mathrm{D}_3, \mathrm{D}_4\}$ to distinguish them.

After detecting malicious nodes, EPIDS will distinguish the types of attacks. The energy comparison results not only indicate the malicious node but also lead us to the types of the attacks. Our scheme partitions the energy comparison results into four domains. The malicious nodes with the energy comparison result E_c, $E_c \in D_i$ is regarded as the node that launched with the DoS attack A_i, $i \in [1, 2, 3, 4]$.

Case 1. $E_c \geq M(E_{Tx} * k + \varepsilon_{amp} * k * d_{\max}{}^2)$, then sensor node *i* is regarded as malicious one launching the *Hello flood* attack.

Case 2. $E_c \leq E_{Tx} * k + \varepsilon_{amp} * k * d_0{}^2$, then sensor node *i* is regarded as malicious one launching the *selective forwarding* attack.

Case 3. $2(E_{Tx} * k + \varepsilon_{amp} * k * d_0{}^2) \leq E\_c \leq (M-1)(E_{Tx} * k + \varepsilon_{amp} * k * d_0{}^2)$, then sensor node *i* is regarded as malicious one launching the *Sybil attack.*

Case 4. $(E_{Tx} * k + \varepsilon_{amp} * k * d_0{}^2) \leq E\_c \leq 2(E_{Tx} * k + \varepsilon_{amp} * k * d_0{}^2)$, then sensor node *i* is regarded as malicious one launching the *Wormhole attack.*

Case 5. $(M-1)(E_{Tx}*k+\varepsilon_{amp}*k*d_0^2)\le E\_c\le M(E_{Tx}*k+\varepsilon_{amp}*k*d_0^2)$, then sensor node i is regarded as malicious one launching the *sinkhole attack*.The printing area is 122 mm × 193 mm. The text should be justified to occupy the full line width, so that the right margin is not ragged, with words hyphenated as appropriate. Please fill pages so that the length of the text is no less than 180 mm, if possible.

5 Simulation and Performance Analysis

We use Network Simulator-2 (NS-2) to evaluate the performance of EPIDS. In order to see how the EPIDS detect the four types of DoS attacks, 100 nodes are randomly deployed in a rectangular field of size (100m×100m). Each node has an Omni-directional antenna having unity gain with a nominal radio range of 25m. The detailed parameters are shown in Table 3.

Table 3. Simulation Parameters

Parameters	Value
Number of nodes	100
Node placement	Random, uniform
Location of the Base station	50, 50
Transmission range	25m
Channel bandwidth	1Mbps
Simulation time	500 seconds
Propagation mode	Free space
Packet size	512bytes
Initial energy of each node	2J

Our security scheme detects various DoS attacks by comparing the energy consumptions and the prediction results of sensor nodes. The average energy consumption of sensor nodes along the time line is shown in Fig.2, where x-axis represents time and y-axis represents the average energy consumptions of sensor nodes.

The line with plus sign (+) represents the average energy consumption of malicious nodes launching *wormhole attacks*. As shown in Fig.2, malicious nodes spend as much as twice the energy than the prediction result in the first 60s. Then they will significantly raise the energy consumption and use up all the 2J energy at the time of 160s, while normal node just consume less than 0.5J energy. The wormhole attack can be easily detected since the wormhole attack spends nearly twice energy than the normal one. EPIDS can detect this abnormal energy consumption before 140s.

The double cross represents the average energy consumed by the nodes launching selective forwarding. The packet drop rate is set to 50%. The difference between the prediction results and the average energy consumption of *selective forwarding* attacks raises after 60s of the simulation, and EPIDS can detect this attack, when there is a difference in energy consumption larger than the preset threshold.

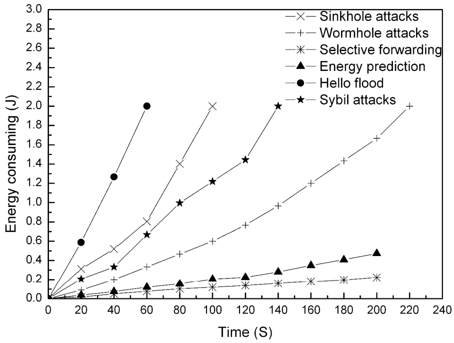

Fig. 2. Comparison of the average energy consumptions of DoS attacks and the predicted result

The star line represents the average energy consumed by the nodes launching *Sybil attacks.* The malicious node would create *M* identities with one real identity and *M-1* fake nodes. These entire *M-1* fake nodes are deployed in other clusters and would be actually controlled by the malicious node that launches the *Sybil attack*. Therefore, the malicious node would spend *M-1* times energy than the predict result. EPIDS can detect this attack when the difference in energy consumption is larger than the preset threshold.

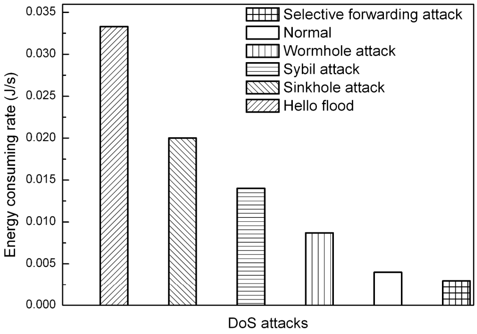

Fig. 3. The energy consumption rate of each DoS attacks

The round dotted line represents the average energy consumed by the nodes launching with *hello flood* attacks. The malicious node maximizes its broadcast range as well as the signal strength. In that case, the energy consumption would be significantly large. As can be seen in Fig.3, the nodes launching *Hello flood* can only operate 60s.

The cross line represents the average energy consumed by the nodes launching *sinkhole attacks.* The malicious nodes attract the communications of cluster heads from the other *M-1* clusters. The difference between the average energy consumption of *sinkhole attacks* and the prediction result increases gradually through the simulation. EPIDS can almost recognize *sinkhole attacks* at the beginning of the simulation. Since the energy consumption is far beyond the prediction result, *Hello flood* attack is the easiest one to be detected.

The energy consumption rate along the DoS attacks is shown in Fig.3. The *Hello flood* attack has the highest energy consumption rate 0.0333 J/s while the *selective forwarding* attack has the lowest energy consumption rate 0.00297 J/s.

Fig.4 shows the detection accuracy ratio with respect to time, where x-axis represents the time and y-axis represents the detection accuracy ratio.

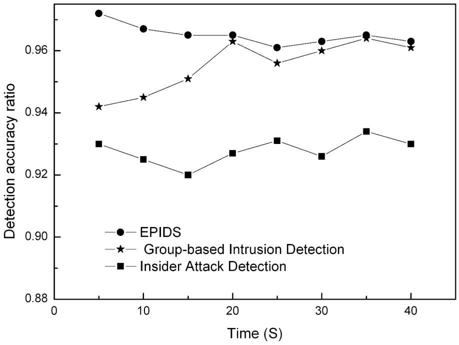

Fig. 4. The detection accuracy rate of DoS attacks

The detection accuracy of the energy prediction-based intrusion detection scheme is much higher than that of the refined group-based intrusion detection scheme. The increase in detection accuracy ratio lies in the fact that malicious nodes have to spend abnormal energy to conduct DoS attacks. This character makes these attacks easier to be detected.

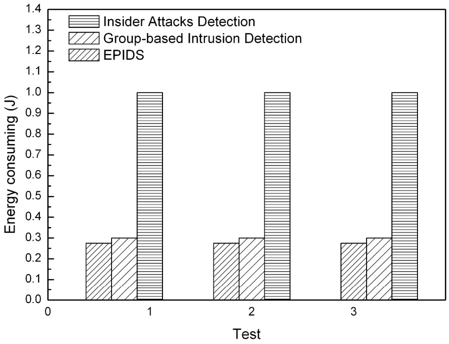

Fig. 5. Comparison of energy consumption among the refined group-based intrusion detection scheme, the insider attacker detection scheme and EPIDS.

Fig.5 shows the comparison of power consumption among the refined group-based intrusion detection scheme, the insider attacker detection scheme and EPIDS. We can see that the EPIDS consumes the least energy than that of the other two intrusion detection schemes. The reason behind this improvement lies in the fact that the energy prediction-based intrusion detection scheme does not require additional monitoring energy which is consumed in the other two schemes throughout the life time of the network.

6 Conclusions

This paper proposes a novel intrusion detection scheme for cluster-based WSNs. The proposed scheme adopts the energy prediction method to detect malicious nodes. Compared with the existing intrusion detection schemes which mainly focus on monitoring the behaviors of malicious nodes, our scheme detects malicious nodes based on the energy character. The results show that the proposed intrusion detection scheme is more efficient in detecting DoS attacks.

Acknowledgments. The work is supported by “the Excellent Master Research Funds for the Hohai University, No. XZX/09B011-02” and “the Fundamental Research Funds for the Central Universities, No.2010B22814, 2010B22914”. and “the research fund of Jiangsu Key Laboratory of Power Transmission & Distribution Equipment Technology, No.2010JSSPD04”. Lei Shu’s research in this paper was supported by Grant-in-Aid for Scientific Research (S)(21220002) of the Ministry of Education, Culture, Sports, Science and Technology, Japan.

References

1. Wang, X., Vasilakos, A., Chen, M., Liu, Y., Kwon, T.: A Survey of Green Mobile Networks: Opportunities and Challenges. ACM/Springer Mobile Networks and Applications (2011)
2. Chen, M., Leung, V., Mao, S., Xiao, Y., Chlamtac, I.: Hybrid Geographical Routing for Flexible Energy-Delay Trade-Offs. IEEE Transactions on Vehicular Technology 58(9), 4976–4988 (2009)
3. Ssu, K.F., Wang, W.T., Chang, W.C.: Detecting Sybil attacks in Wireless Sensor Networks using neighboring information. Computer Networks 53, 3042–3056 (2009)
4. Mohi, M., Movaghar, A., Zadeh, P.M.: A Bayesian Game Approach for Preventing DoS Attacks in Wireless Sensor Networks. In: WRI International Conference on Communications and Mobile Computing, CMC 2009, vol. 3, pp. 507–511 (2009)
5. Krauß, C., Schneider, M., Eckert, C.: On handling insider attacks in wireless sensor networks. Information Security Technical Report 13(3), 165–172 (2008)
6. Wang, Y., Wang, X., Xie, B., Wang, D., Agrawal, D.P.: Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks. IEEE Trans. Mobile Computing 7, 698–711 (2008)

7. Khanum, S., Usman, M., Hussain, K., Zafar, R., Sher, M.: Energy-Efficient Intrusion Detection System for Wireless Sensor Network Based on MUSK Architecture. In: Zhang, W., Chen, Z., Douglas, C.C., Tong, W. (eds.) HPCA 2009. LNCS, vol. 5938, pp. 212–217. Springer, Heidelberg (2010)
8. Li, G., He, J.A., Fu, Y.G.: Group-based intrusion detection system in wireless sensor networks. Computer Communications 31(18), 4324–4332 (2008)
9. Su, W.T., Chang, K.M., Kuo, Y.H.: eHIP: An energy-efficient hybrid intrusion prohibition system for cluster-based wireless sensor networks. Computer Networks 51(4), 1151–1168 (2007)
10. Vullers, R.J.M., Schaijk, R.V., Visser, H.J., Penders, J.H.: Energy Harvesting for Autonomous Wireless Sensor Networks. IEEE Solid-State Circuits Magazine 2(2), 29–38 (2010)