Optimal Activation of Intrusion Detection Agents for Wireless Sensor Networks

Yulia Ponomarchuk and Dae-Wha Seo
Department of Electrical Engineering and Computer Science
Kyungpook National University
Daegu, Republic of Korea
rus_flash@hotmail.com, dwseo@ee.knu.ac.kr

***Abstract*—Recent technological advancements and low price of deployment and maintenance of wireless sensor networks (WSNs) allow their use in numerous applications in industry, research, and commerce, in order to gather environmental data in an unattended manner. Since WSNs usually function in open environments, they may become a target of attacks or malicious activities aiming to gain access to data, manipulate aggregation result, or disrupt the network service. Therefore, intrusion detection becomes crucial for WSNs as a second line of defense. In order to detect "smart" attacks of colluding devices, active monitoring of behaviors of neighboring nodes was proposed, but it is too energy expensive for resource-constrained WSN nodes, making an adaptive technique for activation of intrusion detection system (IDS) agents extremely important. This paper proposed a model for optimal activation of IDS agents for WSNs on the basis of the Ising model.**

Keywords - wireless sensor networks; anomaly detection; intrusion detection system; Ising model

I. INTRODUCTION

WSNs have become one of the most interesting areas of research owing to the recent advancements of technology, low price and easiness of deployment and maintenance, and application flexibility. A common WSN includes a large number of static sensor nodes and one or several base stations (BSs). Sensor nodes are very simple and cheap devices with constrained resources of memory and power, poor processing and communication capabilities. They monitor environment parameters (e.g., temperature, pressure, humidity) and transmit the sensed data in a hop-by-hop manner towards the BS. BSs or sink nodes are usually more powerful and secure, capable of maintaining WSN topology, collecting data from nodes, storing, preprocessing, and sending them to a user or another network, such as Internet.

Commonly, WSNs function in an unattended manner in open environments with easy access. WSN devices communicate via open radio channel and they are prone to occasional network failures, such as HW/SW faults, loss of connectivity, natural disasters [1-4]. Moreover, WSN nodes are vulnerable to a large variety of attacks that may target physical integrity of devices, as well as routing protocols and data, transmitted within the network. Traditional security schemes can not be applied to WSNs directly because of severe resource constraints of nodes and absence of central authority, therefore, new simple, lightweight and efficient algorithms are needed [1, 2, 4]. Moreover, since no security scheme can guarantee that an attacker will not succeed eventually, an IDS is required as a second line of defense. It may detect nodes' anomalous behavior and activate response measures to avoid an assault or minimize its effect on WSN performance. An IDS has to include global agents, responsible for constant monitoring of behaviors of neighboring devices ([5-13]) and node cooperation, because detection of complex attacks of colluding nodes may not be reliable by means of traffic analysis alone. However, this method incurs significant increase of power consumption at a monitoring node, which makes the problem of IDS's self-organization and adaptation extremely important.

In this paper, a model for distributed and adaptive activation of global IDS (GIDS) agents is proposed. It is based on statistical mechanical approach and the Ising ferromagnetic spin model [14-15]. It incurs insignificant computation overheads and small communication costs, since the decision on activation of IDS agents is done locally and there is no need to send all relevant data to the BS. Combined with a reliable traffic analysis technique for local intrusion detection, it is capable of detecting "smart" attacks of colluding devices.

The paper is organized as follows. Section 2 provides description of the problem and brief background information. Section 3 presents the Ising model for activation of GIDS agents. In Section 4, an algorithm for activation of IDS agents is proposed. Section 5, finally, concludes the paper.

II. BACKGROUND

The problem of design of a distributed, lightweight, and efficient IDS for WSNs has been drawing attention of researchers in recent years. Traditional IDSs are classified into network-based (NIDS) and host-based (HIDS) [16]. While HIDS analyzes incoming and outgoing traffic from individual hosts, NIDS is placed at strategic points of the network to analyze the traffic from all devices.

Another approach to IDS classification is based on detection technique: signature or misuse detection, anomaly detection, or specification-based detection [16-17]. *Misuse detection-based* IDSs rely on a priori knowledge of attacks. Therefore, they detect the majority of known intrusions and have rather low false positive rate (number of false alarms). However, new types of assaults can be missed and signature database may require large memory resources. *Anomaly-based* IDSs detect intrusions by comparison of newly acquired traffic profiles to previously created normal profiles.

 ISBN: 978-1-61208-100-7

They are capable of detection of new attacks, but have higher false positive rate, since random network failures are confused with intended assaults. *Specification-based* IDSs use a set of rules or constraints, specific for running protocols and applications. They are considered to be the most suitable for WSNs, since they are able to detect new types of intrusions, have low false positive rate, and require less memory to store specification database.

Significant number of the previously proposed IDSs relies on analysis of incoming and outgoing traffic of a node and monitoring neighbors' behaviors (watchdogs technique) [5-13]. While the former is not energy consuming and can be performed constantly by a local IDS (LIDS) agent, the latter is expensive in terms of energy and memory resources and it is done by a GIDS agent [5, 7-8, 12]. LIDS module detects intrusions against traffic flow in the nearest vicinity, but it is not capable of reliable detection of complex assaults initiated by collaborating malicious devices, which makes GIDS desirable to operate at least on a portion of nodes. Moreover, since any WSN node may be compromised, the network must defend itself from false accusations and GIDS modules may take responsibility for nodes' cooperation and protect a WSN more efficiently. Recent papers on IDS design take this into account and propose algorithms to optimize GIDS deployment and activation [6-8, 12, 18-19]. However, the suggested schemes still require too many nodes to perform overhearing in normal conditions and lack of adaptability.

Techateerawat and Jennings [18] proposed an adaptive activation of IDS agents. When a WSN is not suffering from an attack, the IDS agents are activated according to core, boundary, or distributed defense strategy. As soon as an intrusion is detected, alarm messages are broadcast to activate IDS agents on nodes in the vicinity of an intruder. This results in isolation of the malicious device and limitation of its effect on network performance. This paper proposes an approach to GIDS agents activation, based on the Ising's ferromagnetic spin model [14-15] of statistical mechanics. The Ising model has been used to study critical phenomena in various systems in diverse disciplines, e.g., finance, biology and sociophysics [20]. It is used to describe the collective behavior of an ensemble of interacting components of a complex system, represented by a lattice [15], where each component has a magnetic dipole (spin), e.g., ± 1. It enables modeling local and global influences on constituting components. In [20], the authors proposed to use the Ising model to provide self-organization of a sensor network in detection of pervasive faults. However, the proposed scheme is centralized: the BS aggregates and stores all relevant information and decides, which nodes to activate. This incurs extra communication costs, results in significant time delay, and may lead to problems with scheduling and node synchronization. In this paper, we suggest to use the Ising model to design a distributed and lightweight scheme for optimal and adaptive GIDS agents activation in WSNs.

III. ISING MODEL FORMULATION FOR AN IDS

The Ising model deals with systems, which can be represented as graphs with vertices as interacting components. A common WSN may be considered as a weighted graph with nodes as vertices and links between nodes as edges. Let $G = (V, E, W)$ denote a weighted graph of a WSN, where $V = \{v_i,\ i = \overline{1,N}\}$ is the set of components (sensor nodes), $E = \{(v_i, v_j) \mid v_i, v_j \in V,\ i, j = \overline{1,N}, i \neq j\}$ is the set of edges or possible links between any two nodes, representing interdependences between a pair of components (there are no self-loops), and $W = \{w_{ij} \mid w_{ij} \geq 0,\ i, j = \overline{1,N},\ i \neq j\}$ is a set of weights assigned to edges $(v_i, v_j),\ i, j = \overline{1,N}$ and representing the strength of interaction between nodes v_i and v_j. Thus, each interaction in G is defined by an edge (communication link) and its weight (link quality or trust value). Though G may be a directed graph, in common WSNs nodes change their roles in time course, as well as routing paths. In general, w_{ij} are time dependent, but they are assumed to be constant within a given time interval. Each node $v_i,\ i = \overline{1,N}$, is assigned a spin σ_i, representing the state of its GIDS agent: $\sigma_i = -1$ - GIDS agent is inactive and the node performs only analysis of incoming traffic from neighbors, $\sigma_i = +1$ - GIDS module is active, monitoring and analyzing communication within the radio range.

Given a weighted graph G, a time-dependent Hamiltonian H^{τ} is constructed; it represents the energy in terms of the Ising model:

$$\mathrm{H}^{\tau} = -\sum_{\langle i,j \rangle} w_{ij}\sigma_i\sigma_j - \mathrm{B}^{\tau}\sum_i \sigma_i , \qquad (1)$$

where $\langle i, j \rangle$ denotes pairs of spins σ_i, σ_j of nearest neighbors v_i, v_j; w_{ij} and B^{τ} represent local interactions and external time-dependent field respectively. Since $w_{ij} \geq 0$, nodes tend to have the same state as their neighbors, unless affected by B^{τ}. The assumptions, provided above, correspond to a multicomponent system, where neighbors with anomalous behavior, make a node more likely to change its state from -1 to +1 under similar external influences, which is analogous to ferromagnetic influences of the magnetization model. It should be noted that while the Ising model deals only with binary states of a spin, there are general models, i.e., the Potts model (where a spin may take integer values $\sigma_i = \overline{1,q}$) and the continuous spin models (the XY model and the Heisenberg model) [15], which are considered for further research.

As it was mentioned earlier, external influence of environment is represented by B^{τ}. According to (1), spins tend to line up in the same direction as the external field. In other words, they want to be positive if $\mathrm{B}^{\tau} > 0$ and negative if $\mathrm{B}^{\tau} < 0$. The value B^{τ} at node v_i in time τ can be written as follows:

 ISBN: 978-1-61208-100-7

$$\mathrm{B}^{\tau}(i) = \sum_{k=1}^{N} B_k\left(\mu_k^{\tau}, \left\{\mu_{k_j}^{\tau}\right\}\right)\delta_k(i), \quad (2)$$

where $B_k\left(\mu_k^{\tau}, \left\{\mu_{k_j}^{\tau}\right\}\right)$ is a function that represents external field in the neighborhood of node v_k and depends on the scalar anomaly measure μ_k^{τ} at node v_k and the set of anomaly measures $\left\{\mu_{k_j}^{\tau}\right\}$ of its nearest neighbors v_{k_j}; $\delta_k(i)$ is the Kronecker delta, i.e., $\delta_k(i)=1$ if $k=i$ and $\delta_k(i)=0$ if $k \neq i$. The functional form of $B_k\left(\mu_k^{\tau}, \left\{\mu_{k_j}^{\tau}\right\}\right)$ is taken identical for all nodes v_k, following [20]:

$$B\left(\mu_k^{\tau}, \left\{\mu_{k_j}^{\tau}\right\}\right) = B_0\left(\mu_k^{\tau} + \sum_{k_j} \mu_{k_j}^{\tau} \cdot \exp\left(-\alpha\left|k-k_j\right|\right)\right), \quad (3)$$

where $\left|k-k_j\right|$ represents the distance from node v_k to its neighbor v_{k_j}, α is a weight coefficient for the distance measure, B_0 is a parameter of the function. The value of the anomaly measure μ_k^{τ} is a result of LIDS agent's monitoring of incoming traffic from other devices at node v_k and the set $\left\{\mu_{k_j}^{\tau}\right\}$ represents alerts from its neighbors v_{k_j}.

Given the spin states of nodes and anomaly measures at a given time instant, the problem of self-organization of IDS agents in a WSN is reduced to the estimation of probabilities of the possible subsequent states of the Ising system. Since each spin can take two values, there are 2^N states in total for a graph with N vertices [15]. In order to compute the probabilities of subsequent states, a statistical mechanical approach is used. It is described in the next section.

IV. Optimal Activation of IDS Agents in WSNs

In this section we apply a statistical mechanical approach [14-15] to activation of an IDS, specifically activation and switching off GIDS agents in WSNs. Unlike a typical problem of statistical mechanics, the goal of the proposed model is to estimate probabilities of future thermodynamic states of the system, provided a particular state at time instant τ, not to compute macroscopic parameters (internal energy, the entropy, the specific heat, etc.). The model addresses two problems: it measures the degree of anomaly of traffic flow, using the enhanced version of traffic analysis method [21], and defines the distribution of nodes with active GIDS agents in a WSN.

In terms of statistical mechanics, a thermodynamic state of a system, represented by graph G, is given by the spin states of graph's vertices. The probability P_I of the system being in state I is defined by the Gibbs distribution [14-15]:

$$P_I(\sigma_1,...,\sigma_N) = \frac{1}{Z} e^{-\beta E_I}, \quad (3)$$

where the energy of the state E_I is defined by Hamiltonian H (1), β is proportional to the inverse temperature, and Z is the partition function of the model, defined as the sum:

$$Z = \sum_{\{\sigma_i\}} e^{-\beta \mathrm{H}}. \quad (4)$$

The partition function may be difficult to compute for systems with an irregular lattice and large number of interacting nodes. However, computations are tractable if the simplifying assumptions are made [15].

- The system follows *Markov dynamics*, i.e., the future state depends only on the present state.
- The system has *quasi-static equilibrium* at all time instants, i.e., the probability of transitions between states, having large energy difference is infinitesimal, the system follows single-spin-flip dynamics.
- The system follows the condition of *detailed balance*, i.e., probabilities P_I and P_J of the system being in states I and J respectively and transition probabilities p_{IJ} and p_{JI} are related as:

$$P_I p_{IJ} = P_J p_{JI} \Leftrightarrow \frac{P_I}{P_J} = \frac{p_{JI}}{p_{IJ}}, \quad (5)$$

where $p_{IJ} = p_{JI} \cdot e^{-\beta(E_J - E_I)}$ from (3) and all transition probabilities should satisfy the constraint:

$$\forall I: \sum_J p_{IJ} = 1. \quad (6)$$

Requirements (5-6) allow to break the transition probability into two parts and apply the Metropolis algorithm, the most efficient and widely used for the Ising model [15]:

$$p_{IJ} = g_{IJ} A_{IJ}, \quad (7)$$

where g_{IJ} is the probability that given an initial state I, a new target state J will be generated (selection probability) and A_{IJ} is the acceptance ratio, showing that if the system starts off from state I and the algorithm generates state J from it, the transition will be accepted. In the Metropolis algorithm, selection probabilities are chosen to be equal, resulting in:

$$\forall I \neq J, g_{IJ} = g_{JI} = \frac{1}{N} \Rightarrow \frac{p_{IJ}}{p_{JI}} = \frac{A_{IJ}}{A_{JI}} = e^{-\beta(E_J - E_I)}. \quad (8)$$

According to [15], the optimal algorithm is chosen when

$$A_{IJ} = \begin{cases} e^{-\beta(E_J - E_I)}, & if \;\; E_J - E_I > 0, \\ 1, & otherwise. \end{cases} \quad (9)$$

In other words, if the algorithm selects a state, which has the energy lower than or equal to the present one, such a transition will be always accepted. If a selected state has higher energy, then it may be accepted with the probability, defined by (9). Since each A_{IJ} is strictly positive, the state transition matrix $[A_{IJ}]$ is irreducible.

The change in energy ΔE_i due to a single-spin-flip (from +1 to -1 or vice versa) at a node v_i is defined by (1) and may be rewritten as:

$$\Delta E_i = 2 \sum_{\langle i,j \rangle} w_{ij} \sigma_i \sigma_j - \mathrm{B}^{\tau} \sigma_i , \qquad (10)$$

where $\langle i, j \rangle$ denotes the set of the nearest neighbors v_j of node v_i . Expression (10) shows that areas with traffic anomalies will have higher energy and ensures that more nodes will be able to detect an intrusion. As soon as an anomaly is eliminated, ΔE_i decreases and nodes tend to stop constant monitoring. The flip probability is computed for v_i using (9):

$$p_i^{flip} = \begin{cases} e^{-\beta \Delta E_i}, & if \quad \Delta E_i > 0, \\ 1, & otherwise. \end{cases} \qquad (11)$$

The value p_i^{flip} shows the likelihood of event that node v_i changes its spin $\sigma_i \to -\sigma_i$ under the influence of its neighbors and external field. Initially, all nodes may have the spin $\sigma_i = -1$ and switch to the active GIDS state ($\sigma_i = +1$) with probability p_0 , defined by the minimal number of active GIDS agents over the whole network.

The algorithm for optimal activation of GIDS agents is summarized in Fig. 1. Each node performs it periodically and is able to switch on/off its GIDS agent in dependence on the information from its close neighbors and traffic intensity. There is no need to transmit anomaly measure values to the BS. The weight coefficients are stored at each node.

Algorithm 1: Self-Organization of IDS agents
while (1) do
Collect traffic data
Compute local anomaly measure μ_i^{τ} at current time instant τ and broadcast it to the one-hop neighbors
Compute the external field B_i^{τ} using (2-3)
Compute the change of energy ΔE_i (10) and p_i^{flip} (11)
Change the spin state with probability p_i^{flip}
end

Figure 1. Algorithm for GIDS agents activation, performed by each node.

V. CONCLUSIONS

The paper proposes a model for adaptive optimal activation of GIDS agents for intrusion detection in WSNs. The model is based on the principles of graph theory and statistical mechanics. Given estimations of traffic anomalies, a small fraction of nodes is activated to monitor neighbors behavior, only when it is necessary. Thus, the scheme reduces power consumption due to overhearing and prolongs network's lifetime. The proposed scheme is distributed and lightweight in terms of computation and communication overheads and may be applied in large WSNs, since BSs are not required to gather and store information about all nodes' behaviors. Further research will be devoted to the performance evaluation via simulations and comparison with other strategies for GIDS agents' deployment and activation.

REFERENCES

[1] V.C. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in wireless sensor networks," Journal on Wireless Communications and Mobile Computing, vol. 8, issue 1, 2006, pp. 1-24.

[2] C.Karlof and D.Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Proc. 1st IEEE Int. Workshop on Sensor Network Protocols and Applications, 2003, pp. 113-127.

[3] D.R. Raymond, and S.F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," IEEE Pervasive Computing, vol. 7, issue 1, 2008, pp. 74-81.

[4] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Communications Surveys & Tutorials, v. 8, issue 2, 2006, pp. 2-23.

[5] C. Besemann, S. Kawamura, and F. Rizzo, "Intrusion detection system in wireless ad-hoc networks: Sybil attack detection and others," TechRepublic, 2004, 14p.

[6] I. Chatzigiannakis and A. Strikos, "A decentralized intrusion detection system for increasing security of wireless sensor networks," Proc. IEEE Conf. on Emerging Technologies and Factory Automation (ETFA), 2007, pp. 1408-1411.

[7] T.H. Hai, F. Khan, and E.N. Huh, "Hybrid intrusion detection system for wireless sensor networks," LNCS 4706, Part II, 2007, pp. 383-396.

[8] T.H. Hai and E.-N. Huh, "Optimal selection and activation of intrusion detection agents for wireless sensor networks," Proc. Future Generation Communication and Networking, 2007, vol.1, pp.350-355.

[9] K. Ioannis, T. Dimitrou, and F.C. Freiling, "Towards intrusion detection in wireless sensor networks," Proc. 13th European Wireless Conf., 2007, 7 p.

[10] G. Li, J. He, and Y. Fu, "Group-based intrusion detection system in wireless sensor networks," Computer Communications, vol. 31, issue 18, 2008, pp. 4324-4332.

[11] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," Proc. IEEE Int. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMob'2005), 2005, vol. 3, pp. 253-259.

[12] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," Proc. 3rd IEEE Consumer Communications and Networking Conf., 2006, vol. 1, pp. 640-644.

[13] A.P.R. da Silva, M.H.T. Martins, B.P.S. Rocha, A.A.F. Loureiro, L.B. Ruiz, and H.C. Wong, "Decentralized intrusion detection in wireless sensor networks," Proc. 1st ACM Int. Workshop on Quality of Service & Security in Wireless and Mobile Networks (Q2SWinet'05), 2005, pp. 16-23.

[14] K. Huang, Statistical Mechanics, 2nd ed. Wiley, New York, 1987.

[15] M.E.J. Newman and G.T. Barkema, Monte Carlo Methods in Statistical Physics. Oxford University Press, New York, 1999.

[16] Security in Distributed, Grid, Mobile, and Pervasive Computing, ed. by Xiao Y. Auerbach Publications, CRC Press, 2007.

[17] A. Mitrokotsa and A. Karygiannis, "Intrusion Detection Techniques in Sensor Networks" in Wireless Sensor Network Security, J. Lopez, J. Zhou, Eds. Amsterdam: IOS Press, 2008, pp. 251-272.

[18] P. Techateerawat and A. Jennings, "Energy efficiency of intrusion detection systems in wireless sensor networks," Proc. IEEE/WIC/ACM Int. Conf. on Web Intelligence and Intelligent Agent Technology (WI-IATW), 2006, pp. 227-230.

[19] F. Anjum, D. Subhadrabandhu, S. Sarkar, R. Shetty, "On optimal placement of intrusion detection modules in sensor networks," Proc. 1st Int. Conf. on Broadband Networks, 2004, pp. 690-699.

[20] A. Srivastav and A. Ray, "Self-organization of sensor networks for detection of pervasive faults," Signal, Image nad Video Processing, vol. 4, No. 1, 2010, pp. 99-104.

[21] Yu.V. Ponomarchuk and D.-W. Seo, "Intrusion detection based on traffic analysis in wireless sensor networks," Proc. 19th Annual Wireless and Optical Communications Conf., 2010, pp. 229-235.

 ISBN: 978-1-61208-100-7