2011 International Symposium on Computer Networks and Distributed Systems (CNDS), February 23-24, 2011

A PCA-based Distributed Approach for Intrusion Detection in Wireless Sensor Networks

Mohammad Ahmadi Livani and Mahdi Abadi
Faculty of Electrical and Computer Engineering
Tarbiat Modares University
Tehran, Iran
{ahmadi.l, abadi}@modares.ac.ir

Abstract—**Wireless sensor networks (WSNs) are applied to various applications, ranging from military to civilian fields. Due to the critical nature of such applications, security issues are of significant importance. WSNs are vulnerable to different types of attacks since they are often deployed in hostile and unprotected environments. In this paper, we present a novel distributed intrusion detection approach, called PCADID, for detecting routing attacks in WSNs. In the approach, we partition a WSN into groups of sensor nodes. In each group, some nodes are selected as monitor nodes, which cooperate with each other to compose a global normal profile. Every monitor node establishes a subprofile of its own normal network traffic using principal component analysis (PCA) and sends it to other monitor nodes. Every monitor node composes the global normal profile based upon all received subprofiles and uses it to detect anomalies in its own network traffic. As the normal network behavior changes over time, the global normal profile is updated. We demonstrate that PCADID achieves a high detection rate with a low false alarm rate, while minimizes the communication overhead and energy consumption in the network.**

Keywords-wireless sensor network; distributed intrusion detection; principal component analysis; routing attack

I. INTRODUCTION

Wireless sensor networks (WSNs) have become a growing area of research and development over the past few years. Typically, WSNs are composed of a large number of small sensor nodes that use ad-hoc communications and have limitations in power supply, memory and computational capabilities [1]. WSNs offer a new monitoring and control solution for various applications such as wildlife monitoring, disaster response, traffic monitoring, building monitoring, military surveillance and industrial quality control [2]. Due to the critical nature of such applications, there is a potential risk of attacks on them, either for financial gain or for malicious and illegal purposes. WSNs can play a critical role in detecting these attacks, and thus themselves can become a target for attacks.

Due to the resource limitations of sensor nodes in power supply, memory, and processing power, WSNs are more vulnerable to attacks. Many different types of attacks against these networks have been identified including sinkhole, selective forwarding, wormhole, blackhole and hello flooding attacks [3].

All the security techniques proposed for WSNs can be classified into two main categories: *prevention* and *detection*. Prevention techniques, such as secure routing protocols [4] are usually considered as the first line of defense against attacks. However, we cannot rely on them alone. Detection techniques can come into play once prevention techniques have failed. Generally, there are two types of these techniques: *misuse detection* and *anomaly detection*. A misuse detection technique compares current behavior with known attack signatures and generates an alert if there is a match. An anomaly detection technique detects abnormal behaviors that have significant deviations from a pre-established normal profile. The advantage of anomaly detection techniques is that they do not require known attack signatures and can thus detect novel attacks.

Principal component analysis (PCA) is a powerful technique for analyzing and identifying patterns in data [5]. It finds the most important axis to express the scattering of data. By using PCA, the first principal component (PC) is calculated, which reflects the approximate distribution of data [6].

In this paper, we present a PCA-based centralized approach, called PCACID, and a PCA-based distributed approach, called PCADID, for intrusion detection in WSNs. We partition a WSN into groups of sensor nodes. In each group, some nodes are selected as monitor nodes. In PCACID, every monitor node independently establishes a profile of its own normal network traffic using PCA and uses it to detect anomalous network traffic. The resource limitations of sensor nodes, especially in terms of power supply, memory, and processing power, require a novel and cooperative approach for intrusion detection in WSNs. In PCADID, every monitor node establishes a subprofile of its own normal network traffic using PCA and sends it to other monitor nodes. Every monitor node composes a global normal profile based upon all received subprofiles and uses it to detect anomalous network traffic. In fact, PCADID reduces the memory and energy consumption in the network by distributing the process of establishing and updating the global normal profile among all monitor nodes. We conduct WSN simulations using the NS-2 simulator [7] and consider scenarios for detecting two types of routing attacks.

The rest of this paper is organized as follows: Section II briefly reviews some related work. Section III formally introduces the problem of intrusion detection in a WSN.

Sections IV and V present PCACID and PCADID, respectively. Section VI reports the experimental results and finally Section VII draws some conclusions.

II. Related Work

Many approaches have been proposed for intrusion detection in the traditional networks, but constraints and limitations of WSNs makes direct application of them impossible. In this section, we review some related work in intrusion detection for WSNs.

Loo *et al.* [8] presented a clustering-based approach for intrusion detection in WSNs. Every sensor node uses a fixed-width clustering algorithm to establish a profile of its own normal network traffic and then uses this profile to detect routing attacks. They assume that every sensor node has sufficient power and resources to perform the computation required for intrusion detection. This assumption may not be applicable to all WSNs.

Su *et al.* [9] presented an energy-efficient hybrid intrusion prohibition system, called eHIP, that combines intrusion prevention with intrusion detection to provide a secure cluster-based WSN. The eHIP system consists of authentication-based intrusion prevention subsystem and collaboration-based intrusion detection subsystem. Both subsystems provide heterogeneous mechanisms for different demands of security levels in cluster-based WSNs to improve energy efficiency.

Li *et al.* [10] presented a distributed group-based intrusion detection approach that combines the Mahalanobis distance measurement with the OGK estimators to take into account the inter-attribute dependencies of multi-dimensional sensed data. In the approach, they first partition the sensor nodes in a WSN into a number of groups such that the nodes in a group are physically close to each other and their sensed data are similar enough. The monitor nodes supervise sensed data in each group in turn to average the power consumption among the group members. If an obvious deviation between monitored sensed data is found, an alarm will be issued.

Wang *et al.* [11] presented an anomaly detection technique based on fuzzy C-means clustering (FCM) that can be used to detect routing attacks in WSNs.

III. Problem Definition

We consider a WSN composed of a large number of small sensor nodes deployed in a target field. We partition the network into a number of groups. The sensor nodes within the same group are physically close to each other and use a suitable routing protocol so that they can route messages among themselves. The partitioning of the network could be static or dynamic [10]. In dynamic partitioning, the network may be dynamically rearranged periodically, if the environmental conditions change.

In each group G, some sensor nodes are selected as monitor nodes. At each time interval Δ_k, every monitor node $m_i \in G$ extracts a feature vector x_{ik} from its own network traffic. Each feature vector is comprised of a set of attributes or features.

At each time window t, the monitor node m_i collects a matrix $X_i(t)$ of feature vectors from its own network traffic:

$$X_i(t) = \begin{bmatrix} x_{i1}(t) \\ x_{i2}(t) \\ \vdots \\ x_{in_i}(t) \end{bmatrix}, \quad (1)$$

where n_i is the number of feature vectors.

Our aim is to detect routing attacks launched by compromised or malicious nodes. These attacks are detected by identifying anomalous feature vectors.

IV. Centralized Approach

In this section, we present a centralized approach, called PCACID, for intrusion detection in WSNs. The approach consists of two phases: *training* and *detection*.

A. Training Phase

The training phase involves establishing a profile of normal network traffic. Let $X_i(0)$ be an $n_i \times d$ matrix of feature vectors collected by a monitor node $m_i \in G$ from its own normal network traffic. Each feature vector $x_{ik}(0) \in X_i(0)$ is comprised of a set of features:

$$x_{ik}(0) \in \Re^d, \quad (2)$$

where d is the number of feature. Notice that the length of each feature vector is the same for all monitor nodes.

m_i first normalizes $X_i(0)$ to a range [0,1] [12] and then computes the column-centered matrix of it:

$$\hat{X}_i(0) = (I - \frac{1}{n_i} e_{n_i} e_{n_i}^T) X_i(0) = X_i(0) - e_{n_i} \bar{x}_i^T(0), \quad (3)$$

where $\bar{x}_i(0)$ is the column means of $X_i(0)$ and $e_{n_i} \equiv (1, 1, ..., 1)^T$ is a vector with the length n_i. The principal components (PCs) of $X_i(0)$ are given by a singular value decomposition (SVD) [13] of $\hat{X}_i(0)$:

$$\hat{X}_i(0) = U_i(0) \Sigma_i(0) V_i^T(0), \quad (4)$$

where $V_i(0)$ is the matrix of PCs of $X_i(0)$ and $\Sigma_i^2(0)$ is the diagonal matrix of eigenvalues ordered from largest to smallest. The first PC of $X_i(0)$ is denoted as $\varphi_i(0)$.

Afterward, m_i calculates the projection distance of each feature vector $x_{ik}(0) \in X_i(0)$ from $\varphi_i(0)$ (See Fig. 1):

$$d_p(x_{ik}(0), \varphi_i(0)) = (\| x_{ik}(0) - \bar{x}_i(0) \|^2 - (\varphi_i^T(0) \cdot (x_{ik}(0) - \bar{x}_i(0)))^2)^{\frac{1}{2}} \quad (5)$$

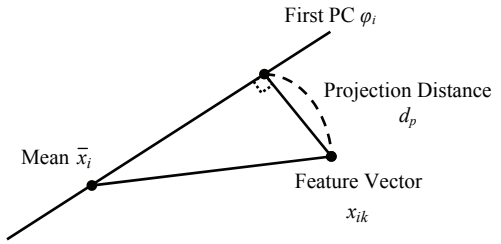


Figure 1. Projection distance of a feature vector x_{ik} from the first PC φ_i

The maximum projection distance of all feature vectors $x_{ik}(0)$ from $\varphi_i(0)$ is calculated as

$$d_{i,\max}(0) = \max\left\{d_p(x_{ik}(0), \varphi_i(0))\right\}, k = 1 \ldots n_i \tag{6}$$

Finally, m_i uses the triple $(\bar{x}_i(0), \varphi_i(0), d_{i,\max}(0))$ to establish the normal profile $P_i(0)$.

B. Detection Phase

The detection phase involves identifying anomalous feature vectors. Let $X_i(t)$ be a matrix of feature vectors collected by the monitor node m_i from its own network traffic at time window t. m_i detects anomalous feature vectors based upon the normal profile established in the training phase. To do this, it first calculates the projection distance of each feature vector $x_{ik}(t) \in X_i(t)$ from $\varphi_i(t-1)$ and then classifies $x_{ik}(t)$ as anomaly, if the calculated projection distance is greater than $d_{i,\max}(t-1)$:

$$\begin{cases} d(x_{ik}(t), \varphi_i(t-1)) > d_{i,\max}(t-1) & : \text{Anomaly} \\ d(x_{ik}(t), \varphi_i(t-1)) \le d_{i,\max}(t-1) & : \text{Normal} \end{cases} \tag{7}$$

Since the normal network behavior may change over time, the simple use of a predefined normal profile will not be efficient. Hence, it is necessary to every monitor node to update its normal profile.

Let t be the current time window and $XN_i(t)$ be the set of normal feature vector collected at the ρ previous time windows (See Fig. 2):

$$XN_i(t) = \bigcup_{\tau=t-\rho}^{t} nv(X_i(\tau)), \tag{8}$$

where $nv(X_i(\tau))$ is the set of feature vectors classified as normal at time window τ.

To update the normal profile, m_i first calculates the first PC $\varphi_i(t)$ and then calculates the maximum projection distance of all normal feature vectors $x_{ik}(t) \in XN_i(t)$ from $\varphi_i(t)$:

$$d_{i,\max}(t) = \max\left\{d_p(x_{ik}(t), \varphi_i(t))\right\}, k = 1 \ldots |XN_i(t)| \tag{9}$$

Finally, m_i uses the triple $(\bar{x}_i(t), \varphi_i(t), d_{i,\max}(t))$ to update the normal profile $P_i(t)$.

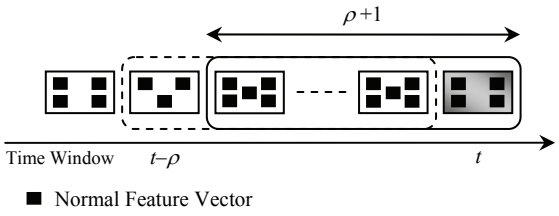


Figure 2. Updating the normal profile. The gray box represents the set of normal feature vectors at current time widow t

V. Distributed Approach

The resource limitations of sensor nodes, especially in terms of power supply, memory, and processing power, require a novel and cooperative approach for intrusion detection in WSNs. In this section, we present a distributed intrusion detection approach, called PCADID, which reduces the memory and energy consumption in the network by distributing the process of establishing and updating the normal profile among all monitor nodes. The approach consists of two phases: *training* and *detection*.

A. Training Phase

In the training phase, every monitor node $m_i \in G$ establishes a subprofile of its own normal network traffic and cooperates with other monitor nodes to compose a global normal profile. To do this, we divide the set of network traffic features F into a number of subsets and assign each subset $f_j \in F$ to a monitor node:

$$F = \bigcup_j f_j \tag{10}$$

Let f_j be the subset of features assigned to m_i and $X_i^j(0)$ be an $n_i \times d_j$ matrix of feature vectors collected by m_i from its own normal network traffic. Each feature vector $x_{ik}^j(0) \in X_i^j(0)$ is comprised of a set of features:

$$x_{ik}^j(0) \in \Re^{d_j}, \tag{11}$$

where $d_j = |f_j|$ is the number of features assigned to m_i.

m_i first normalizes $X_i^j(0)$ to a range [0,1] [12] and then uses (3)-(6) to establish a normal subprofile $P^j(0)$:

$$P^j(0) = \left\{(\bar{x}^j(0), \varphi^j(0), d_{\max}^j(0))\right\}, \tag{12}$$

where $\bar{x}^j(0)$ and $\varphi^j(0)$ are the column means and first PC of $X_i^j(0)$. $d_{\max}^j(0)$ is the maximum projection distance of all feature vectors $x_{ik}^j(0) \in X_i^j(0)$ from $\varphi^j(0)$.

Afterwards, m_i sends $P^j(0)$ to its one-hop neighbor monitor node. After a monitor node has received normal subprofiles from its neighbor monitor node, it sends them with its own normal subprofile to other monitor nodes along a logical ring, as illustrated in Fig. 3.

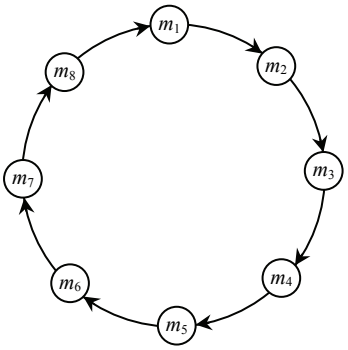


Figure 3. A logical ring constructed by eight monitor nodes

Finally, m_i composes the global normal profile $GP(0)$ based upon all normal subprofiles.

$$GP(0) = \bigcup_j P^j(t) = \bigcup_j \{(\bar{x}^j(0), \varphi^j(0), d^j_{\max}(0))\}, \quad (13)$$

B. Detection Phase

In the detection phase, during each time window t, every monitor node $m_i \in G$ collects an $n_i \times d$ matrix $X_i(t)$ of feature vectors from its own network traffic and detects anomalous feature vectors based upon the global normal profile established in the training phase. Each feature vector $x_{ik}(t) \in X_i(t)$ is divided into a number of sub-feature vectors:

$$x_{ik}(t) = \bigcup_j x^j_{ik}(t), \quad (14)$$

where $x^j_{ik}(t)$ is a sub-feature vector corresponding to the subset of features f_j.

Then, m_i calculate the projection distance of each sub-feature vector $x^j_{ik}(t) \subseteq x_{ik}(t)$ from $\varphi^j(t-1) \in GP(t-1)$ and classifies $x_{ik}(t)$ as anomaly, only if the calculated projection distance is greater than $d^j_{\max}(t-1)$.

Since the normal network behavior may change over time, a predefined global normal profile will not be sufficiently representative for future anomaly detection. Hence, at the end of each time window t, every monitor node $m_i \in G$ updates its subprofile and cooperates with other monitor nodes to update the global normal profile $GP(t)$.

VI. Experiments

A. Simulation Enviroment

In order to evaluate the performance of PCACID and PCADID, we simulated some attacks on WSNs. Our simulation was based on the sensor network package from the Naval Research Laboratories [14], running on the NS-2 simulator [7]. We extended the simulation package to implement two types of attacks: active sinkhole attack and passive sinkhole attack. The simulated WSN consisted of 25 sensor nodes, one base station, and one phenomenon node. We used IEEE 802.11 as the MAC layer protocol and AODV as the routing protocol. We deployed the sensor network over a 500(m) × 500(m) field. We also partitioned the sensor nodes into three groups, and in each group, two sensor nodes were selected as monitor nodes (See Table I).

TABLE I. Simulation Parameters

Simulation Time	10000(s)
Number of Sensor Nodes	25
Number of Monitor Nodes in a Group	2
MAC Layer Protocol	MAC 802.11
Routing Protocol	AODV
Transport Layer	Constant Bit Rate
Puase Time	0.01(s)
Maximum Mobility	5(m/s)
Maximum Bandwidth	2(Mbps)
Simulation Area	500(m) × 500(m)

We should identify suitable traffic features that are useful for detecting routing attacks, while attempting to have as few features as possible. This is because more features means more computation time and more energy consumption are incurred by the sensor nodes. Hence, we used fourteen features, presented in [6] and [8], and divided them into two subsets. The first subset consisted of ten features and the second one consisted of six features.

B. Simulated Attacks

We now introduce routing attacks that we simulated in our experiments:

1) Active Sinkhole Attack: A malicious node attracts all network traffic from sensor nodes in a particular area towards itself. When the malicious node receives a broadcasted RREQ packet for a route to the destination, it immediately sends a false RREP packet, which contains the maximum destination sequence number and minimum hop count. So, neighboring nodes assume that the malicious node is having the best route towards the destination.

2) Passive Sinkhole Attack: This attack is similar to the active sinkhole attack. The only difference is that instead of sending a false RREP packet, the malicious node starts the attack by broadcasting a false RREQ packet.

C. Experimental Result

The simulation time was set to 10,000(s). The length of the training phase was set to 1000(s) and the collected feature vectors were used to establish the normal profile. A malicious node launched active sinkhole attack from 5000(s) to 7000(s) and passive sinkhole attack from 3500(s) to 6000(s). The length of each time interval was set to 5(s) and the length of each time window was set to 250(s).

Cumulative percent variance (CPV) [15] is a measure of the percent variance captured by the first few PCs. It can be used to evaluate the importance of each PC. Fig. 4 shows the percent variance captured by each PC in PCACID. As shown in the figure, the first PC only explains 45.61% of the total variance.

Fig. 5 shows the percent variance captured by each PC in PCADID for two subsets of traffic features. As shown in the

figure, the first PCs of the subsets explain 80.96% and 61.08% of the total variance, respectively. This shows that the first PC in PCADID can express the scattering of data better than that of in PCACID and thus can establish a better profile of normal network traffic.

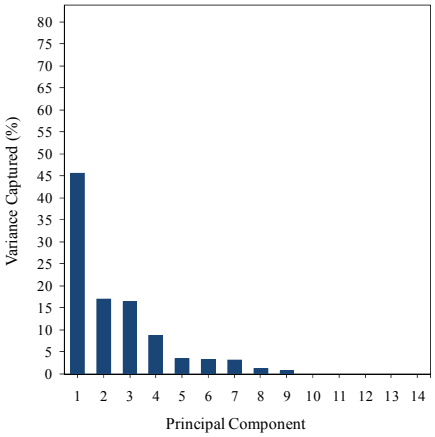
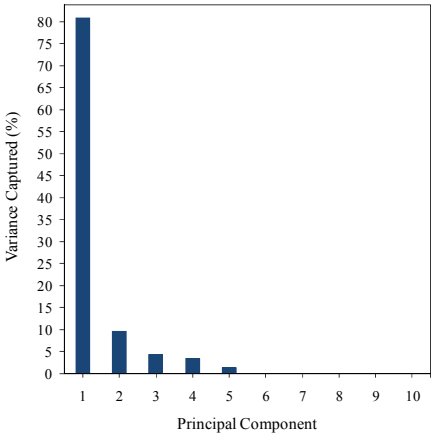
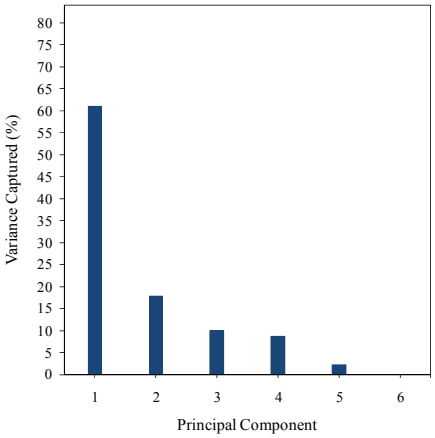


Figure 4. The percent variance captured by each PC in PCACID



(a) First subset of traffic features



(b) Second subset of traffic features

Figure 5. The percent variance captured by each PC in PCADID for two subsets of traffic features

End-to-end delay refers to the time taken for a packet to be transmitted across a network from source node to destination node. Routing attacks degrade the performance of a WSN by injecting false routes into the network. Fig. 6 shows the impact of active sinkhole attack on the average end-to-end delay as the performance parameter.

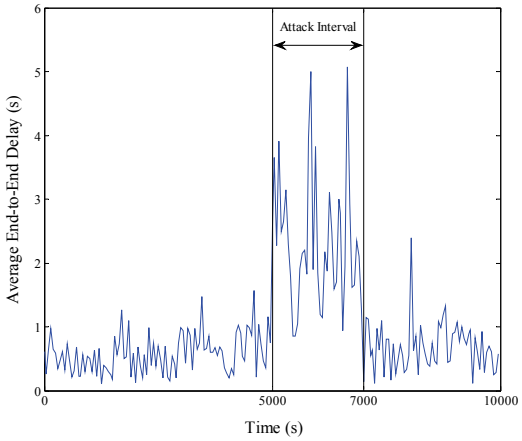


Figure 6. Impact of active sinkhole attack on the average end-to-end delay

We used two performance measures: *detection rate* (*DR*) and *false alarm rate* (*FAR*). The detection rate is defined as the percentage of anomalous feature vectors that are successfully detected. The false alarm rate is defined as the percentage of normal feature vectors that are incorrectly detected as anomaly.

Fig. 7 compares the average detection and false alarm rates of PCACID and PCADID for different values of ρ = 10, 8, 6, 4, 2. As the figure shows, if we decrease the number of pervious time windows when updating the normal profile, the false alarm rate will be increased. This shows that it is necessary to consider the previous normal feature vectors to keep the normal profile from being too sensitive to the sudden changes in the network.

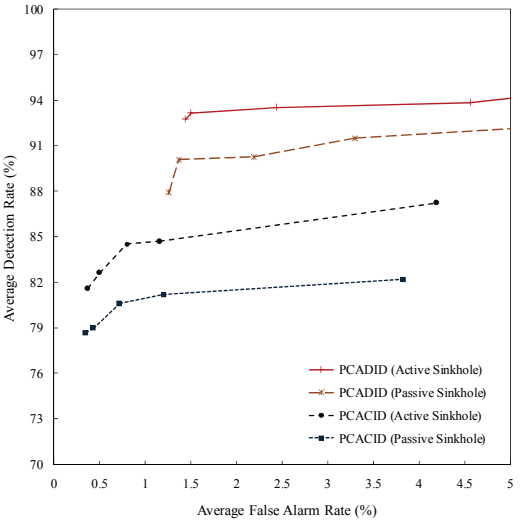


Figure 7. Comparison of the performance of PCACID and PCADID for different values of ρ

Table II compares the performance of PCACID and PCADID with and without updating of the normal profile. As it can be seen in this table, the average detection and false alarm rates for PCACID with updating are 80.81% and 0.46%, respectively; while for PCACID without updating, these rates are 77.78% and 0.39%, respectively. In addition, the average detection and false alarm rates for PCADID with updating are 91.63% and 1.43%, respectively; while for PCADID without updating, these rates are 85.08% and 1.31%, respectively. Hence, we conclude that PCACID and PCADID achieves a better performance when we keep the normal profile updated. In the experiment, the parameter ρ was set to 8.

TABLE II. COMPARISON OF THE PERFORMANCE OF PCACID AND PCADID WITH AND WITHOUT UPDATING OF THE NORMAL PROFILE

Routing Attacks	**PCACID**				**PCADID**			
	With Updating		***Without Updating***		***With Updating***		***Without Updating***	
	DR%	***FAR%***	***DR%***	***FAR%***	***DR%***	***FAR%***	***DR%***	***FAR%***
Active Sinkhole	82.63	0.50	80.17	0.13	93.16	1.50	86.63	1.50
Passive Sinkhole	79.00	0.43	75.40	0.65	90.10	1.37	83.54	1.13
Average	80.81	0.46	77.78	0.39	91.63	1.43	85.08	1.31

VII. CONCLUSIONS

In this paper, we presented a PCA-based centralized approach, called PCACID, and a PCA-based distributed approach, called PCADID, for intrusion detection in WSNs. We partition a WSN into groups of sensor nodes. In each group, some nodes are selected as monitor nodes. In PCACID, every monitor node independently establishes a profile of its own normal network traffic using PCA and uses it to detect anomalous network traffic. In PCADID, every monitor node establishes a subprofile of its own normal network traffic using PCA and sends it to other monitor nodes. Every monitor node composes a global normal profile based upon all received subprofiles and uses it to detect anomalous network traffic. In fact, PCADID reduces the memory and energy consumption in the network by distributing the process of establishing and updating the global normal profile among all monitor nodes.

We conducted WSN simulations using the NS-2 simulator and considered scenarios for detecting two different types of sinkhole attack. The simulation results showed that PCADID achieves a better performance than PCACID, while minimizes the memory and energy consumption in the network. Also, PCADID significantly performs better than PCADID without updating in terms of detection and false alarm rates.

ACKNOWLEDGEMENTS

This work was supported in part by the Iran Telecommunication Research Center (ITRC) under contract 88-12-128.

REFERENCES

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, August 2008.

[2] C.-Y. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, August 2003.

[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113–127, AK, USA, May 2003.

[4] J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, "Security for sensor networks," in *Proceedings of the CADIP Research Symposium*, Baltimore, MD, USA, October 2002.

[5] M. Ahmadi Livani and M. Abadi, "An energy-efficient anomaly detection approach for wireless sensor networks," in *Proceedings of the 5th International Symposium on Telecommunications*, Tehran, Iran, December 2010.

[6] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "Dynamic anomaly detection scheme for AODV–based mobile ad hoc networks," *IEEE Transaction On Vehicular Technology*, vol. 58, no. 5, pp. 2471–2481, June 2009.

[7] NS-2: The Network Simulator. http://www.isi.edu/nsnam/ns/

[8] C. 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, December 2006.

[9] W. Su, K. Chang, and Y. Kuo, "eHIP: an energy–efficient hybrid intrusion prohibition system for cluster-based wireless sensor networks," *Computer Networks*,vol. 51, no. 4, pp. 1151–1168, March 2007.

[10] G. Li, J. He, and Y. Fu, "Group-based intrusion detection system in wireless sensor networks," *Computer Communications*, vol. 31, no. 18, pp. 4324–4332, December 2008.

[11] T. Wang, Z. Liang, and C. Zhao, "A detection method for routing attacks of wireless sensor network based on fuzzy C-means clustering," in *Proceedings of 6th International Conference on Fuzzy Systems and Knowledge Discovery*, vol. 3, pp.445–449, Tianjin, China, August 2009.

[12] M. Ahmadi Livani and M. Abadi, "Distributed PCA-based anomaly detection in wireless sensor networks," in *Proceedings of the 5th International Conference for Internet Technology and Secured Transactions*, London, UK, November 2010.

[13] G. H. Golub and C. F. Van Loan, *Matrix Computations*, Third Edition, Johns Hopkins University Press, 1996.

[14] I. Downard, "Simulating sensor networks in NS-2," *Technical Report Naval Research Laboratory*, Washington DC, USA, May 2004.

[15] I. T. Jolliffe, *Principal Component Analysis*, Second Edition, New York: Springer-Verlag, 2002.