Hindawi Publishing Corporation
Journal of Electrical and Computer Engineering
Volume 2014, Article ID 245938, 6 pages
http://dx.doi.org/10.1155/2014/245938

Research Article

CUSUM-Based Intrusion Detection Mechanism for Wireless Sensor Networks

Bishan Ying

Wasu Media Network Co., Hangzhou 310012, China

Correspondence should be addressed to Bishan Ying; yingbishan_cn@126.com

Received 12 December 2013; Accepted 30 December 2013; Published 11 February 2014

Academic Editor: Xue Chen

The nature of wireless sensor networks (WSNs) makes them very vulnerable to adversary's malicious attacks. Therefore, network security is an important issue to WSNs. Due to the constraints of WSN, intrusion detection in WSNs is a challengeable task. In this paper, we present a novel intrusion detection mechanism for WSNs, which is composed of a secure data communication algorithm and an intrusion detection algorithm. The major contribution of this paper is that we propose an original secure mechanism to defend WSNs against malicious attacks by using the information generated during data communication. The approach is able to protect the data communication in a WSN even if some sensor nodes are compromised by adversary. The proposed approach is easy to be implemented and performed in resource-constrained WSN. We also evaluate the proposed approach by a simulation experiment and analyze the simulation results in detail.

1. Introduction

Wireless sensor networks (WSNs) are systems that comprise large numbers of wirelessly connected and spatially distributed sensor nodes across a large field of interest [1]. There is a wide range of applications where the WSNs are extensively used, and their development in other applications is still growing. However, the intrinsic nature of WSNs makes them vulnerable to malicious attacks. An adversary can physically compromise a subset of sensor nodes in a WSN to eavesdrop or destroy information. The malicious nodes (or compromised nodes) become *black holes* in a WSN [2]. Therefore, network security is a very important issue to WSNs. Generally speaking, network security techniques can be divided into two categories: prevention-based techniques and detection-based techniques. When an intrusion takes place, prevention-based techniques are the first line of defense against attacks, while detection-based techniques aim at identifying and excluding the attacker after the fail of prevention-based techniques. Detection-based techniques can be grouped into two categories: misuse detection and anomaly detection. Misuse detection techniques match patterns of well-known attack profiles with the current changes, whereas anomaly detection uses established normal profiles and detects unusual deviations from the normal behavior as anomalies [3].

An intrusion detection system (IDS) monitors a host or network for suspicious activity patterns outside normal and expected behavior [4]. Currently, there are a number of research efforts on intrusion detection for WSN. Although intrusion detection is an important issue to WSN, the research on intrusion detection for WSNs is still preliminary [5]. Due to some intrinsic features of WSN, it is difficult to perform efficient intrusion detection in such a resource-restricted environment. Many intelligent or statistical approaches are too complex for WSNs. Therefore, due to the constraints of WSN, IDS in WSNs is challengeable and need more effort to be done in this direction.

In this paper, we present a novel intrusion detection mechanism for WSNs, which is composed of a secure data communication algorithm and an intrusion detection algorithm. The major contribution of this paper is that we propose an original secure mechanism to defend WSNs against malicious attacks by using the information generated during data communication. The approach is able to protect the data communication in a WSN even if some sensor nodes are compromised by adversary. We provide a relatively simple but reliable approach to support secure data communication

in WSN. The remaining of the paper is organized as follows. In Section 2, we first introduce the network model for this study. Then we illustrate how to construct secure path for data communication in WSN and how to perform data communication via secure paths in Section 3. In Section 4, we propose a CUSUM-based intrusion detection algorithm for WSN by using the path information generated during data communication. In Section 5, we evaluate the performance of the proposed approach by simulation. Section 5 gives an overview of the related works. Section 6 concludes the paper with an outlook to future research directions.

2. Network Model

Generally, a WSN [6, 7] is a network composed of a large number of sensor nodes that are equipped with environmental sensors for temperature, pH value, humidity, and so forth and can communicate with each other through a wireless radio device. A typical WSN consists of two types of nodes: sink nodes and sensor nodes. The sink, also known as base station, is a powerful node that behaves as an interface between the sensor nodes and the clients of the network. The sensor nodes, also known as motes or simply nodes are small and resource-constrained devices that have the ability of sensing the surrounding environment. Sensor nodes in WSN are always densely deployed either inside the phenomenon or very close to it. Although WSNs belong to the general family of wireless ad hoc networks, they have several distinctive features of their own [8]. For example, a sensor node in WSN is small and inexpensive device with constrained transmit power and energy supplies.

In this paper, we consider a very simple WSN model for illustrating the approach. Assume that there are k nodes in the network. Each sensor node in this WSN is battery-powered and has limited sensing, computation and wireless communication, capabilities. In this network, the sink is a data communication center equipped with sufficient computation and storage capabilities. Sensor nodes generate sensor data and aggregate data packets. The sink allocates the data from sensor nodes periodically. There are a small number of malicious nodes in the WSN. Assume that the number of the malicious nodes is h ($0 < h \ll k$).

We assume that malicious nodes, in order to allay suspicions, selectively drop only a small proportion of all packets passing by rather than every packet. The routing layer of WSNs is threatened by various attacks. However, due to the focus of our paper, it will not be further discussed and here we consider only selective forwarding attacks throughout this paper.

3. Normal-Path-Based Data Communication

Data communication in WSN is a process of data packet relay from the source to the sink. If the packet arrives at the sink successfully at the end, it means that there are no (or few) malicious nodes on the path. Therefore, we can make use of such feature to improve the quality of the subsequent data communication and perform intrusion detection. In this section, we present a normal-path construction (NPC) algorithm for this purpose. In this algorithm, we assume that if a data packet from the source successfully arrives at the sink, the path from the source to the sink is more likely to be secure for subsequent data communication. The details of the algorithm are illustrated as follows (see Figure 1).

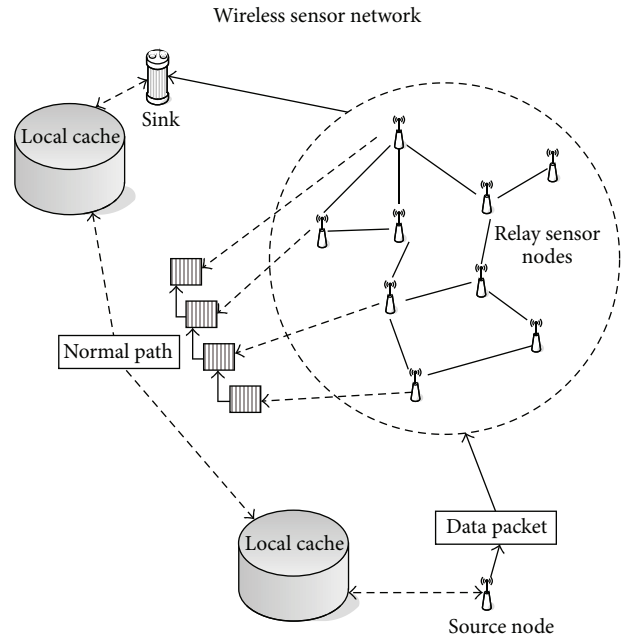

Figure 1: The architecture of the NPC algorithm for secure data communication in WSN.

(1) A source node (A) sends a data packet to the sink (S). To each data packet, A appends an empty list (L) to it.

(2) When a sensor node (R_k) receives a packet, if it is a normal node, it adds its identity (d_k) to L. It is possible that malicious nodes will also take this action in order to disguise themselves.

(3) On the arrival of the packet, S extracts $L = \{d_1, d_2, \ldots, d_n\}$ (here d_i refers to the identity of a relay sensor node R_i) from the packet and stores it in its local cache. Here L is called a *normal path* in this case.

(4) S adds L to a notification packet and sends the packet to A. The sensor nodes in L are used as the relay nodes.

(5) When a relay sensor node (R_j) receives the notification packet, if its identity d_j is involved in L, it extracts a subpath $L_j = \{d_{j+1}, d_{j+2}, \ldots, d_n\}$ from L and stores it into its local cache. R_j extracts its next-hop node (R_{j-1}) with identity d_{j-1} from L and forwards the packet to it.

(6) On the arrival of the notification packet, A extracts L from the packet and stores it into its local cache.

In this algorithm, each normal sensor node adds its identity to the data packet during the process of data communication. When the packet reaches the sink finally, it involves a routing path that consists of a list of the identities

of *normal* sensor nodes (here *normal* does not mean the node is a normal node but a node that behaves normally). It means that the path is potentially secure for data communication and can be used by the source node (also the other nodes on the path) again in the future. A complete normal path is always terminated and allocated by the sink. Here we use a *notification mechanism* to tell the source node that requires the path for future data communication. The sink sends back a notification packet that contains a normal path to the source node. The task of notification may be performed at intervals rather than immediately in order to reduce the overall cost of the network. We can formally denote a normal path as a triple $\langle A, L, \Delta T\rangle$, where A is the source node for the path, L is the identity list, and ΔT denotes the trust value for a normal path with an initial value λ ($\lambda > 0$). The larger the ΔT is, the more secure the path is.

As long as a source node receives enough normal paths from the sink, it is able to send data via these paths. When a source node (A) intends to send a data packet to the sink, it first checks its local cache. If there are normal paths, it selects a normal path $\langle A, L, \Delta T\rangle$ with the largest trust value from its local cache. The data packet from A will be sent to the sink along the path. If the packet is dropped or does not reach the sink within the required time slot, it means that there may exist malicious nodes on the path. A just decreases the trust value of the path by 1. If the trust value of a normal path is cleared up, A will remove it from its local cache. We can see that a normal path is not secure for data communication all the time. Normal paths are evaluated according to their quality of service (QoS) for data communication periodically. We deal with the problem of selective forwarding by using an accumulated trust mechanism. We can exclude malicious nodes from data communication as many as possible by using this mechanism.

4. Intrusion Detection Based on Path Information

4.1. Malicious Path Construction. As we have mentioned before, the normal-path algorithms are based on the assumption that if a data packet from a source node successfully arrives at the sink, the path from the source to the sink is more likely to be secure for subsequent data communication. On contrary, if a data packet from the source fails to reach the sink, it means that there is at least a malicious node on the path from the source to the sink. According to the definition of normal path, we just attach each normal path with a trust value. When the trust value for a normal path decreases to zero or negative value, the path will be removed from the local cache of sensor nodes. We define such a removed path as *malicious path*, compared to normal path.

The malicious path construction (MPC) algorithm is illustrated as follows.

(1) For a given normal path $\langle A, L, \Delta T\rangle$, check its trust value ΔT at time slot t.

(2) If $\Delta T > 0$, use the path for data communication and then go to step 1.

(3) If $\Delta T \leq 0$, remove the path from the local cache and mark the path as malicious path.

(4) Add the malicious path to a collection.

Malicious paths are also the by-product of data communication in WSN, similarly to normal path. Unlike normal path, malicious path reflects a more definite status for WSN, because a malicious path is generated due to data communication failures. Therefore, we can make use of malicious paths to perform intrusion detection for WSN. An intuitive assumption is that the nodes which appear in more malicious paths are more likely to be malicious nodes. Therefore, we can record malicious paths in data communication and count the appearance frequency for each node. We can treat the nodes with high frequency as malicious nodes.

4.2. CUSUM-Based Intrusion Detection. In this section, we illustrated a novel intrusion detection mechanism based on malicious paths. We propose to use change-point detection to detect the change point of sensor node behavior in WSN. A sequential and nonparametric CUSUM algorithm [9] with light computation load is used to support intrusion detection for WSN. CUSUM can detect sharp but continuous increase. The major procedure of detection is as follows.

(1) Let X_n be the number of malicious paths that the node appear in within a sampling time Δn and $\overline{X}$ the mean value of random sequence $X = \{X_1, X_2, \ldots, X_n\}$.

(2) Let $Z = \{Z_1, Z_2, \ldots, Z_n\}$ with β, where $Z_n = Z_n - \delta$ and δ is the peak value of normal behaviors for a specific WSN status so that all elements of Z are negative and so is $\overline{Z}$.

(3) Then, we have the following equations:

$$\begin{aligned} S_n &= \sum_{i=0}^{n} Z_i, \quad S_0 = 0, \\ Y_n &= S_n - \min_{0\leq i\leq n} S_i, \\ Y_n &= \left(Y_{n-1} + Z_n\right)^+, \quad Y_0 = 0, \\ x^+ &= \begin{cases} x, & x > 0, \\ 0, & x \leq 0. \end{cases} \end{aligned} \tag{1}$$

(4) When a change happens, such as when insider attack occurs, Z_n will suddenly increase to positive. $Y_t > h$, for some t, indicates that an attack possibly starts where k is the smallest n and h is the threshold of abnormal WSN statics. Δt is then considered as the change point of node behaviors. The decision function at Δt, say, $d(Y_t)$, is given as follows:

$$d\left(Y_t\right) = \begin{cases} 1, & \text{if } Y_t > h, \\ 0, & \text{else.} \end{cases} \tag{2}$$

Here h is the threshold value for an attack. The value of one indicates that an attack occurs, while the value of zero shows that the WSN runs normally.

Table 1: The basic network setting for the simulation.

Parameters	Value
Node number	100
Drop ratio	0.2
Number of malicious nodes	10
Initial trust value (λ)	3

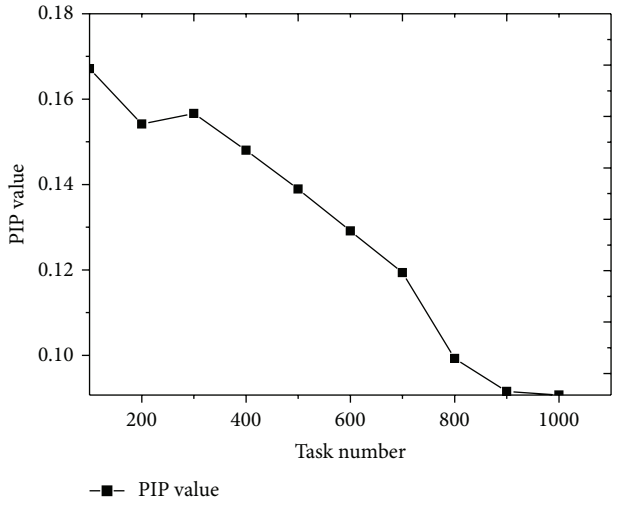

Figure 2: The PIP value for the method under different number of tasks.

In this way, we can perform intrusion detection by analyzing malicious paths. This operation can be done in the sink with the most volume of malicious paths. However, we can also distribute the task of intrusion detection to sensor nodes with enough malicious paths.

5. Simulation and Evaluation

In this section, we construct simulation to evaluate the performance of the proposed approach. The major metric for performance evaluation is the *packet interception probability* (PIP) for a source node, defined as the ratio of the number of intercepted data packets to the total number of packets sent from the source node. The basic setting for the simulation is given in Table 1. Assume that there are 100 sensor nodes in the WSN and there are a small number of malicious nodes in the network. Here the parameter *drop ratio* refers to the probability that a malicious node will drop a data packet.

We first fix the number of the malicious nodes in the WSN to 10 and investigate the PIP for a given source node. Figure 2 depicts a plot of the PIP for the source node under different collection of data communication tasks. We can see that the PIP value of the WSN decreases when the number of data communication tasks increases. When the number of tasks is small, there are not enough normal paths and malicious paths. Therefore, the PIP value is very high at the beginning. It makes sense that we can get more normal paths for secure data communication and malicious paths for intrusion detection when we perform more data communication tasks in the WSN. Therefore, the PIP value goes down quickly when we perform enough tasks.

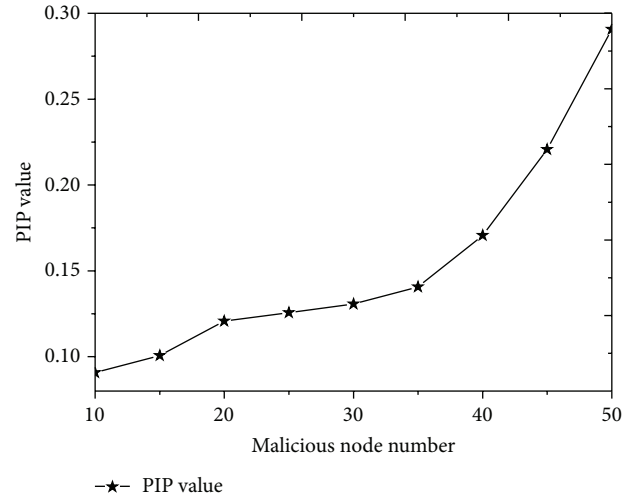

Figure 3: The PIP value for the method under different number of malicious nodes.

Then we change the number of the malicious nodes to see the performance of PIP. For each number of malicious nodes, we perform a certain number (about 1000) of data communication tasks for the source node and evaluate the average PIP for the source node. Figure 3 shows a plot of the PIP for the source node under different numbers of malicious nodes. It can be seen that the method can support secure data communication when the number of the malicious nodes is not very large, from 10 to 35. The number of the malicious node increases, but the PIP value does not go up obviously. It makes sense that the method can detect and exclude malicious nodes from data communication when the number is not very large. However, when the number increases from 40 to 50, the PIP value goes up heavily. As there are so many malicious nodes in the WSN, it is impossible to preserve secure data communication in this case.

6. Related Works

Although intrusion detection has been studied a lot in traditional networks and computer systems [10, 11], Intrusion detection for WSNs is an emerging research field. There have been some ongoing efforts in this field. WSNs are threatened by various attacks. Here we mainly talk about the intrusion detection methods for the attacks with tampering or packet dropping. Most of the existing approaches against tampering attacks are based on encryption. However, encryption cannot solve the problem of packet dropping.

Da Silva et al. in [12] proposed a methodology to construct a decentralized IDS for WSNs. The network behavior is generated from the analysis of the events detected at the specific monitor node, which is responsible for monitoring its one-hop neighbors looking for malicious nodes. However, this kind of distributed IDS will cause a high overhead to resource-constrained WSNs. Su et al. in [13]

have presented an energy-efficient hybrid intrusion prohibition system for cluster-based WSNs. The system is comprised of authentication-based intrusion prevention subsystem and collaboration-based intrusion detection subsystem. The member node monitoring mechanism is performed at the cluster head and limited to the detection of compromised nodes through the used pairwise key only. Yu and Xiao in [14] have proposed an approach for detecting selective forwarding attacks in WSN. Their scheme makes use of a multihop acknowledgement method to launch alarms by obtaining responses from intermediate nodes. However, their approach mainly relies on acknowledgement between nodes. They do not consider the situation that the malicious nodes may drop the alert packets of both sensor nodes and the sink during intrusion detection. Lee et al. in [15] proposed a specification based intrusion detection mechanism for the LEACH protocol. However, their method can only be used in a specific protocol for WSNs. Loo et al. in [16] have presented an anomaly-based intrusion detection scheme that was used to detect network level intrusions. They use a clustering algorithm to build the model of normal network behavior, and then use this model to detect anomalies in traffic patterns for the network. Shaikh et al. in [17] addressed that the problem of malicious nodes in WSN could send faulty anomaly and intrusion claims about the legitimate nodes to the other nodes to destroy the secure mechanism of the whole network. Therefore, they have proposed a validation algorithm that utilized the concept of intrusion-aware reliability to provide adequate reliability at a modest communication cost. However, their approach does not deal with the attacks with tampering or packet dropping in WSN.

Compared with existing works in this field, our approach uses a novel notification mechanism, which makes full use of the data communication process of WSN, to perform lightweight intrusion detection. The algorithms are easy to be implemented and performed in resource-constrained WSN. The advantage of our approach is that the normal paths and malicious paths are constructed as a by-product of data communication and can be reused in subsequent data communication.

7. Conclusion

In this paper, we propose a novel intrusion detection method for secure data communication in WSN. The key component of the approach is a novel notification mechanism, which makes full use of the data communication process of WSN, to support lightweight intrusion detection. The advantage of our approach is that the normal paths and malicious paths are constructed as a by-product of data communication and can be used to support secure data communication. The process of constructing normal path or malicious path places limited consumption on sensor nodes and WSN. Compared with existing works in this field, the algorithms of our approach are not very complex for the computing and storage ability of sensor nodes. According to the result of simulation, the performance of the proposed approach is reasonable and acceptable. In all, our work tries to take step forward intrusion detection for WSN.

Future works may include (1) improving the efficiency of the algorithms to reduce the overhead of path notification; (2) considering the case that the number of malicious nodes dynamically changes; (3) considering a more complex WSN model to evaluate the approach.

Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work is partially supported by the National Development and Reform Commission, China, under special grants of "The Operation System of Multimedia Cloud Based on the Integration of Telecommunications Networks, Cable TV Networks and the Internet."

References

[1] K. S. Low, W. N. Win, and M. J. Er, "Wireless sensor networks for industrial environments," *Materials Science Forum*, vol. 119, pp. 83–87, 1992.

[2] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–105, 2002.

[3] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM '00)*, pp. 275–283, August 2000.

[4] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[5] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2–23.

[6] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[7] K. Ioannis, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in *Proceedings of the 13th European Wireless Conference*, 2007.

[8] 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, August 2005.

[9] B. E. Brodsky and B. S. Darkhovsky, *Nonparametric Methods in Change-Point Problems*, Kluwer Academic, Boston, Mass, USA, 1993.

[10] Z. G. Chen and S. Wang, "Minimax probability machine with genetic feature optimized for intrusion detection," *Information Technology Journal*, vol. 7, no. 1, pp. 185–189, 2008.

[11] Z. Muda, W. Yassin, M. N. Sulaiman, and N. I. Udzir, "A K-Means and Naive Bayes learning approach for better intrusion detection," *Information Technology Journal*, vol. 10, no. 3, pp. 648–655, 2011.

[12] A. P. R. Da Silva, A. A. F. Loureiro, M. H. T. Martins, L. B. Ruiz, B. P. S. Rocha, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in *Proceedings of the 1st ACM International Workshop on Quality of Service and Security*

in Wireless and Mobile Networks (Q2SWinet '05), pp. 16–23, ACM, New York, NY, USA, October 2005.

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

[14] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," in *Proceedings of the 20th International Parallel and Distributed Processing Symposium (IPDPS '06)*, 2006.

[15] S. Lee, Y. Lee, and S. Yoo, "A specification based intrusion detection mechanism for the LEACH protocol," *Information Technology Journal*, vol. 11, no. 1, pp. 40–48, 2012.

[16] C. E. 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, 2006.

[17] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y. Song, "Intrusion-aware alert validation algorithm for cooperative distributed intrusion detection schemes of wireless sensor networks," *Sensors*, vol. 9, no. 8, pp. 5989–6007, 2009.