Energy Efficiency of Intrusion Detection Systems in Wireless Sensor Networks

Piya Techateerawat, Andrew Jennings
School of Electrical and Computer Engineering
RMIT University, Melbourne, Australia
s3100474@student.rmit.edu.au, ajennings@rmit.edu.au

Abstract

Security is a significant concern for many sensor network applications. Intrusion detection is one method of defending against attacks. However, standard intrusion detection is not suitable for sensor networks with limited battery power, memory and processing resources. This paper compares several approaches to intrusion detection in sensor networks. We investigate accuracy of detecting attacks, versus energy efficiency.

1. Introduction

Sensor networks are developed for deployment at locations without infrastructure support. It may provide a solution to many applications, for example traffic, environment and pollution monitoring [1], [2].

With this purpose there are strong restrictions on energy consumption, computing resources and memory size. It is also important to keep cost per unit as low as possible [3].

Security of sensor networks is limited by wireless nature, network structure and resources. It is expected that the network is flexible and adaptable to the addition of new nodes, and provide for routing changes in the event of node failure. The most critical aspect of sensor network application is energy efficiency [4], [5], [6], [7].

An Intrusion Detection System (IDS) detects a security violation on a system by monitoring and analyzing network activity. There are two approaches: misuse detection and anomaly detection. Misuse detection identifies an unauthorized use from signatures while anomaly detection identifies from analysis of an event. When both techniques detect violation; they raise an alarm signal to warn the system [8], [9], [10], [11].

Related Work The distributed monitor was first developed by Kachirski and Guha in the context of Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks [12]. Our implementation of the distributed defense method is largely based on their approach. Newcome and et al. also discuss security in sensor network [6], [13], [14].

Contributions This paper investigates new approaches to intrusion detection, based on the layout and selection of monitoring nodes. In the default, every sensor node in the network could monitor, but this makes for poor energy efficiency. An analysis is based on the response of intrusion detection nodes, number of required alert messages and intruder detection ability. We also explore these in the context of different size of network clusters.

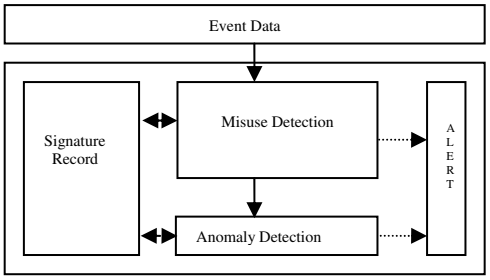

Figure 1. Intrusion Detection System framework

2. Intrusion Detection System

Intrusion Detection System (IDS) uses either anomaly detection or misuse detection. This paper uses a decision mechanism derived from Siraj and et al. [10], [15], [16]. Within IDS, tasks are combined to minimize energy consumption. So, anomaly detection is proceeding while event data is pre-checked for misuse detection. The signature records are combined to a single database to reduce memory use. In the normal situation, both systems operate with same record.

Event Data is the network activities (for example number of success and failure of authentication). This set of data is prepared for further analysis.

Misuse Detection analyses event data from signature record. In case of event data is matched with any rules, alert signal will be raised. Otherwise, event data is forwarded to anomaly detection for further analysis.

Anomaly Detection compares event data with signature record to find harmful attacks from intruder. If probability reaches the risk threshold, alert signal will be raised.

Signature Record is a database which contains signature of unauthorized and high risk activities. In addition, each record contains level of harm for misuse detection and probability chance for anomaly detection.

Alert is an interface between operating system and IDS. Duties of alert are broadcasting alarm and alert information.

Proceedings of the 2006 IEEE/WIC/ACM International Conference on
Web Intelligence and Intelligent Agent Technology (WI-IAT 2006 Workshops)(WI-IATW'06)
0-7695-2749-3/06 $20.00 © 2006 IEEE

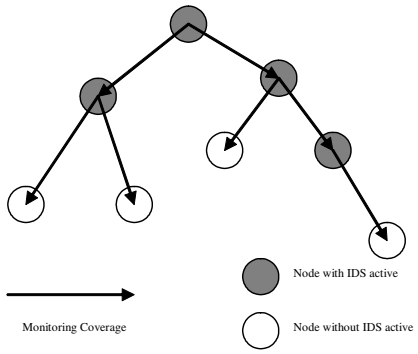

Figure 2. Agent node selection in tree hierarchy

3. Selection of intrusion detection nodes

In this paper, three strategies have been investigated. These are core defense, distributed defense and boundary defense. Each of these strategies operates within a cluster of nodes.

Core defense involves selecting IDS nodes around a centre point. It assures that no intruders break into a central station in each cluster. This model defends from the most inner point then strikes back to the outer area.

Boundary defense selects nodes along a boundary at the perimeter of the cluster. It focuses on preventing an intruder from breaking into the cluster from outside the cluster.

Distributed defense has an agent node selection algorithm which is developed from the voting algorithm [12]. IDS node selection follows a tree hierarchy. A voting system is employed [13], [14].

The voting algorithm for the selection of nodes in distributed defense consists of 4 steps: vote preparation, voting, vote counting and activate IDS. There are two parameters in this algorithm. First, number of hop count determines the threshold of selection for the number of hops between a candidate node and itself. A larger hop count means less activated nodes and each IDS node has to take responsibility for more nodes. Second, the voting threshold is the minimum number of votes before activating IDS. The procedure lets each node elect its own gateway. The stages are:

1. **Vote Preparation**: Each node decides their gateway or nearest node. A hop count parameter determines distance between agent node and neighboring nodes.
2. **Voting**: Each node transmits their vote message to their gateway.
3. **Vote Counting**: To count a received vote.
4. **Activate IDS**: If the number of votes exceeds the threshold, then activates IDS. The node will remain active until timeout, at which point the process 1-4 will be commenced again.

Table 1. Simulation result from core attack

Total Node	Type of Defence	IDS nodes when Alarm	No. of broadcast Alarm Message
10	core	10	109
20	core	19	239
40	core	27	599
80	core	29	1239
10	voting	8	109
20	voting	16	419
40	voting	27	1639
80	voting	55	3298
10	border	10	89
20	border	18	339
40	border	10	639
80	border	20	1429

4. Simulation

We set up a simulation to analyze the three defense models. A network topology has been created with a central station at a centre point in each cluster. Only designated nodes operate to monitor traffic. There are 3 defense strategies; boundary, distributed and core defense. Table 1 shows a number of simulated attacks with the various node selection approaches. The simulation covers 10-80 nodes in each cluster and simulates 3 types of defenses. In the results, it shows a number of alarm messages and active nodes. This also represents the energy consumption.

In simulation, we develop IDS nodes in Ptolemy software which includes a sensor network package. In this package, it contains a sensor network operation and communication component. So, we create IDS software which performs on top of sensor network operation and voting function for distributed defense. Then, we set up attack messages which trick nodes into reading wrong sensing data. In message contents, we follow the rules of communication messages but modify some contents and format at random times. Therefore attacker transmits near real communication message which report inaccurate sensing data. The numbers of attackers are based on simulation models and cluster sizes.

IDS mechanism detects unusual behavior from incorrect format. In case an incorrect packet is not related to transmission error (for example an incorrect node id), it raises an alarm signal to prepare for intruders. Then a group of activated nodes will be surrounded the intruders to protect from breaking into network.

A scenario with same cluster size used the same deployment for the result consistency. The nodes have been deployed randomly for each different cluster size as shown in Fig. 3. The result also has been evaluated from average outcome from each scenario as in Table 1.

5. Analysis

According to the results, when there are less than 20 nodes in a cluster, it shows a good detection rate while alert numbers shows no difference in all strategies. An alert node is a neighbor node which receives alert

Proceedings of the 2006 IEEE/WIC/ACM International Conference on
Web Intelligence and Intelligent Agent Technology (WI-IAT 2006 Workshops)(WI-IATW'06)
0-7695-2749-3/06 $20.00 © 2006 IEEE

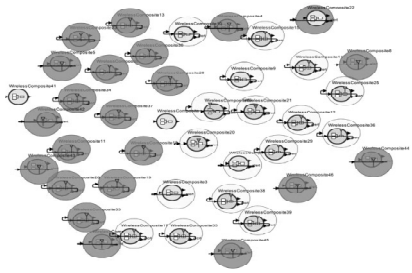

Figure 3. Node deployment (greyed node is IDS activated)

message from agent node, and then activates its IDS software to prepare for attack. In the attack, the broadcast messages increase when the number of nodes increases. When number of nodes is greater than 20, the alert messages increases dramatically in an exponential curve. The distributed defense results in a broadcast of approximately 300% more messages than the core defense with 80 nodes as shown in Fig. 4 (a). So, the energy consumption at alert time is increasing as the cluster size increases. The reason that distributed defense has more alert messages is agent node selection spreads the selected nodes over the area. So, selected nodes cover more area than other strategies, and have more neighbor nodes. Since an alert message goes to a number of neighbors, the greater coverage results in more alert messages being broadcast. Fig. 4 (a) shows the number of messages generated. Fig. 4 (b) shows a ratio of the number of alerted nodes and the total number of nodes in the network.

In the core defense strategy, the ratio drops dramatically when the number of node increases. Also, at 80 nodes, boundary and inner area attack drop under 0.1. However, core defense is not able to detect a boundary attack and inner area attack in large cluster size. Since, an agent node has not spread to outer or covers a border line. Therefore its alert node ratio drops down for a larger cluster. Energy consumption in core defense is very low when number node is increasing. However, it suffers from false negatives.

The boundary defense also demonstrates ratio reduction in a large network cluster. However, boundary attack on large cluster has not reduced in the same manner as inner or core attack because it has more opportunity to detect intruder on border line with boundary defense. As shown in Fig. 4 (d), the number of nodes is increasing but the alert node ratio is decreasing. Therefore average energy consumption is reduced when cluster size is larger but the tradeoff is false negatives in core and inner attack.

Table 2 shows a response of each attacks and defenses. The result shows the weaknesses of core defense which boundary and inner attack are missed. Boundary defense misses on core and inner attack in large cluster. While distributed defense always detects an attack on different part of network cluster.

Table 2. Table shows results of defense for each attack and cluster size. (O is Detected; X is Missed)

Total Node	Type of Defense	Core Attack	Inner Attack	Boundary Attack
10	Core	O	O	O
	Distributed	O	O	O
	Border	O	O	O
20	Core	O	O	O
	Distributed	O	O	O
	Border	O	O	O
40	Core	O	O	**X**
	Distributed	O	O	O
	Border	**X**	O	O
80	Core	O	**X**	**X**
	Distributed	O	O	O
	Border	**X**	**X**	O

6. Discussion

Activating every node to operate IDS software, wastes energy. Consequently, it is important to minimize the number of selected nodes to run intrusion detection. We consider three approaches. The boundary defense has strong response in border line and core defense is strong in core area. Distributed defense can respond equally to entire network but number of broadcast alert message is the highest.

According to the results, a small cluster size can manage with all defense strategies and provide no difference in energy consumption. In large cluster size, each defense model has its own advantages and disadvantages. However, distributed defense is energy intensive for large clusters. The simpler schemes of boundary and core defense are much more economical in their use of energy. However, they are vulnerable to attack from within the cluster.

7. Conclusion and Future work

Boundary defense reduces the number of IDS nodes. It also keeps broadcast alert messages to a minimum. However, when intruder attacks on core area or inner part, it shows a large number of false negatives in a larger cluster.

The least number of broadcast messages is for core defense. However, this has limited coverage. Core defense has strong defense in the inner network. The broadcast message is largely as same as boundary defense. This strategy has to wait for intruder to reach the core area then it raises alert signal to strike back. However, boundary attack and inner area have weaknesses, and a node can be captured without notice.

Distributed defense has developed from agent node selection algorithm which spreads an agent to entire network area. It is able to respond to all attackers from small to a large cluster. However, the weakness is the sharply increasing of alert messages when cluster size is

Proceedings of the 2006 IEEE/WIC/ACM International Conference on
Web Intelligence and Intelligent Agent Technology (WI-IAT 2006 Workshops)(WI-IATW'06)
0-7695-2749-3/06 $20.00 © 2006 IEEE

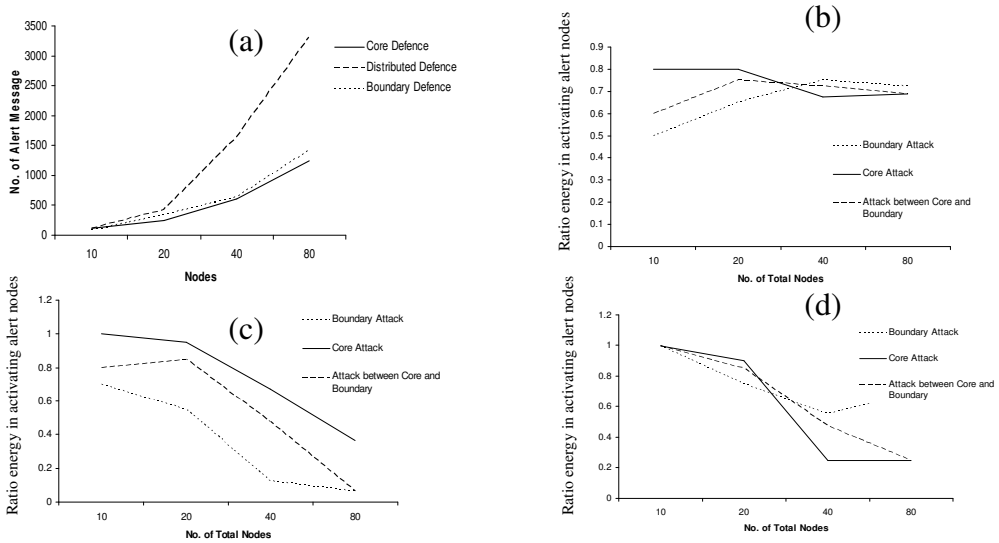

Figure 4. (a) Number of alert message in each defense. (b) Ratio energy in activating alert nodes and total nodes in distributed defense (c) Ratio energy in activating alert nodes and total nodes in core defense. (d) Ratio energy in activating alert nodes and total nodes in boundary defense.

larger. To improve detection performance, we pay a high penalty in energy consumption.

Given the complementary advantages of the two schemes, it is natural to think of hybrid schemes that combine the best attributes. Future work will consider a dynamic defense strategy of agent node in environment to suit each particular situation. Given that nodes can turn on IDS fairly quickly, it is natural to consider adaptive strategies in responding to the threat as it develops. However there is the disadvantage of added coordination costs. We investigate whether a dynamic approach is superior to static defense.

8. Acknowledgment

The research work describes in this paper builds on the result of Ptolemy II with extensive tools.

9. References

[1] A. Dunkels, T. Voigt, N. Bergman and M. Jonsson. "The Design and Implementation of an IP-based Sensor Network for Intrusion Monitoring", *Swedish National Computer Networking Workshop*, Nov 2004

[2] C. Murthy and B. Manoj. *Ad Hoc Wireless* Networks, E^{d} 1st, Prentice Hall PTR, United States of America, 2004, pp. 204-219

[3] A. Hac. *Wireless Sensor Network Designs*, E^{d} 1st, Wiley, Great Britain, 2003, pp. 213-234

[4] A. Perrig, J. Stankovic and D. Wagner. "Security in Wireless Sensor Networks", *Communications of the ACM*, vol. 47, pp 53-57, Jun 2004

[5] E. Shi and A. Perrig. "Designing Secure Sensor Networks", *IEEE Wireless Communications*, pp. 38-43, Dec 2004

[6] J. Newcome, E. Shi, D. Song and A. Perrig. " The Sybil Attack in Sensor Networks: Analysis & Defenses", *Information Processing in Sensor Networks 2004*, pp. 259-268, Apr 2004

[7] J. Deng, R. Han and S. Mishra. "Security Support for In-Network Processing in Wireless Sensor Networks", *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pp. 83-93, 2003

[8] B. White and L. Huson. "A Peer-Based Hardware Protocol for Intrusion Detection Systems", *Military Communications Conference 1996*, vol. 2, pp. 468-472, Oct 1996

[9] D. Mutz, G. Vigna and R. Kemmerer. "An Experience Developing an IDS Stimulator for the Black-Box Testing of Network Intrusion Detection Systems", *Computer Security Applications Conference, 2003.Proceedings. 19th Annual 2003*, pp. 374-383, 2003

[10]A. Siraj, S. Bridges and R. Vaughn. "Fuzzy Cognitive Maps for Decision Support in an Intelligent Intrusion Detection System", *IFSA World Congress and 20th NAFIPS International Conference 2001*, vol. 4, pp. 2165-2170, Jul 2001

[11]S. Northcutt and J. Novak. *Network Intrusion Detection*, E^{d} 3rd, New Riders Publishing, United State of America, 2002, pp. 339-395

[12]O. Kachirski and R. Guha. "Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks", *Proceeding of the IEEE Workshop on Knowledge Media Networking*, pp. 153-158, 2002

[13]J. Balasubramaniyan, J. Garcia-Fernandez, D. Isacoff, E. Spafford, D. Zamboni, "An architecture for intrusion detection using autonomous agents*," Computer Security Applications Conference, 1998, Proceedings., 14th Annual* , vol., no.pp.13-24, 7-11 Dec 1998

[14]S. Snapp, J. Brentano, G. Dias, T. Goan, L. Heberlein, C. Ho, K. Levitt and B. Mukherjee , *A System for Distributed Intrusion Detection*, COMPCON Spring '91 Digest of Papers, San Francisco, CA, March 1991, pp. 170-176.

[15]T. Ohta and T. Chikaraishi. "Network Security Model*", International Conference on Information Engineering 1993* , vol 2, pp. 507-511, 1993

[16]J. Tao, L. Jiren and Q. Yang "The research on Dynamic Self-Adaptive Network Security Model", *International Conference on Technology of Object-Oriented Language and Systems*, pp. 134-139, 2000