Study on Intrusion Detection Policy for Wireless Sensor Networks

Jiang Xu[1], Jin Wang[1], Shengdong Xie[1], Wenliang Chen[2] and Jeong-Uk Kim[3]

[1]*School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China*
[2]*College of Mechanical Engineering, Nanjing University of Aeronautics & Astronautics, Nanjing 210016, China*
[3]*Department of Energy Grid, Sangmyung University, Seoul 110-743, Korea*

Abstract

In recent years, wireless sensor networks applications are increasing very fast such as battle field, disaster recovery, environmental monitoring and healthcare etc. To secure these networks, a secure and efficient system is required to avoid such networks from attacks. In this paper, an intrusion detection policy is proposed for wireless sensor networks. It monitors the communication between neighboring nodes and finds those nodes that are not working normally. Some general rules are defined to detect such nodes called compromised nodes. Simulation results are provided to analyze the performance of the proposed policy which validate that our policy performs better in terms of higher intrusion detection rate and receives lower false positive rate.

Keywords: *Wireless sensor networks, intrusion detection policy, security, specification based*

1. Introduction

Intrusion detection system (IDS) provides better security to the network in case of inside attacks [1]. An adversary compromises the legitimate node in inside attack to perform malicious activities. A compromised node may affect the network by launching different kind of various attacks [2]. Some of these attacks are homing, flooding, selective forwarding, black-hole, sink-hole, worm-hole etc. Bojkovic, et al., briefly discuss a number of attacks that influence the overall working of wireless sensor networks [3]. According to them, IDS can provide a better security solution for these kinds of attacks.

Detection policy is a systematic approach to identify compromised node(s) in the network. There are three types of detection policies; misuse detection, anomaly detection and specification based detection. In misuse detection, the system searches for some specific patterns or signatures to detect the intruder while in an anomaly detection; system learns about the normal behavior of the network and then declares anything that deviates from a specified pattern that it has learnt. Rules are made in specification based detection for particular attacks to analyze the behavior of the nodes. If it violates n numbers of rules, it is declared as abnormal.

Wireless sensor networks (WSNs) are easily installable in an area called sensor field [4]. There are number of applications of WSNs such as battle field surveillance, disaster recovery, health-care, tracking animal movement, environmental monitoring as well as understanding volcano condition etc. The networks are composed of small size sensor nodes which are densely deployed in the sensor field. Usually, those sensors have little computational power

and small size memory. The authors in [5, 6] favor specification based detection method for sensor nodes. Misuse detection and anomaly detection are rather computationally expensive as well as take more memory. IDS based security mechanisms are considered as a frontline to secure network from different threats. In [7], the authors discussed various IDS based security schemes in and explored them the way they apply detection policy.

In this paper, we propose an intrusion detection policy for WSNs. It can also detect transport layer attacks and several routing layer attacks. There is a data collection unit that listens to the network in promiscuous mode. This unit transmits that data to data processing unit. Data processing unit processes the collected data to populate audit lists. Detection policy finds abnormal activity of nodes by comparing their current behavior with the threshold values.

2. Related Work

In [8], the authors propose a specification based distributed centralized security mechanism that is well known in the research field of intrusion detection systems for wireless sensor networks. It works in three phases; data acquisition, rule application and intrusion detection. During rule application phase, monitor node applies rules for various attacks such as exhaustion attack, selective forwarding, black hole attack and flooding attack etc. The authors in [9] have modified the detection algorithm according to their layered model.

In [5], the authors introduce a neighbor monitoring technique called spontaneous watchdog. They favor specification based detection scheme for WSNs over other detection techniques.

A distributed centralized detection technique is discussed in [10]. It detects three types of attacks by an anomaly detection algorithm called Cumulative Summation. These are: 1) compromised node attracts the attention of other nodes; 2) affect the data of the messages; 3) compromised node floods packets to exhaust resources of other nodes. Due to the reason that CUSUM algorithm is not simulated or tested, it is rather difficult to analyze the effectiveness of this algorithm.

A specification based cooperative local auditing mechanism to detect selective forwarding and black-hole attack is presented in [1]. They discuss about the possibility of the sink-hole attack in MintRoute routing protocol [11]. They extend their previous work and added rules for detecting the sink-hole attack as well. In [6], they have formulated lightweight distributed intrusion detection architecture (LIDeA). It is installed in all the sensor nodes and cooperates with each other to locate compromised nodes.

3. Our Intrusion Detection Policy

Sensor node works in an infrastructure-less and dynamic environment. It performs various tasks according to its configuration. It is a self control device that works independently without any direct interaction of human user. It can be compromised by an adversary to perform malicious activities. Currently, there is not any complete security framework that secures wireless sensor network from these kinds of inside attacks. Intrusion detection schemes are considered more effective to detect abnormal behavior of nodes that degrade the overall performance of the network [12].

Regarding intrusion detection policies, rules are defined to detect the abnormal behavior of the nodes. It is favored among other two schemes because misuse detection mechanism cannot find unknown attacks whereas anomaly detection approach is expensive. We propose an intrusion detection policy for securing wireless sensor networks from different kinds of attacks. Rules are not formalized for any particular routing protocol. They are kept general and can be tested for any routing protocol. The proposed scheme is discussed below.

3.1. Data Collection

Sensor nodes usually listen to the communication between neighboring nodes that reside in its radio range. Here data collection unit simply listens to these packets and transmits them to data processing unit. It does not store these packets and just act like a channel between outside world and inner detection body.

3.2. Data Processing

Several IDS based security mechanisms apply their detection scheme after promiscuous listening of messages. Our detection strategy is also inspired from these ideas. In data processing unit, whenever a packet is received from data collection unit, its header is interpreted to analyze the actual transaction and values are updated in audit data list (A_List). It is the list that holds the data that is used by detection policy unit. The general format of this list is shown in Table 1.

Table 1. Audit Data List (A_List)

Node_ID	Packet Sent	Packet Received	Packet Forward	Packet Retransmit
X	X1	X2	X3	X4
Y	Y1	Y2	Y3	Y4

Consider a node A which senses a packet. It interprets the header. Let it is sent by node X to node Y. So node A updates it's A_List against packet sent and packet received field of node X and node Y respectively. Now, suppose node Y forwards that packet. Hence, packet forward of node Y and packet receive against the recipient node will be updated.

Node_ID is indexed by taking the hash of actual ID and other fields are populated respectively. Let a fixed size array data structure is used for N_List than a suitable hash function helps to place the values and retrieve too. It might be expensive with respect to memory but efficient with respect to computation. In best case the computation time complexity is O (1). The worst case time complexity deals in the way hashing mechanism is handled i.e. open chaining etc.

A_List is updated for each instance of the surroundings. The length of A_List depends on the number of neighboring nodes from which the particular node is listening messages. Hence, we can make some assumption about the length of A_list if we know the density of the network. It is clear from the above discussion of A_List that packet is not stored but some fields of every packet are checked and packet is finally discarded.

The above process continues for some time t epoch. After this, A_List is refined by removing the data of those nodes that are already declared as malicious. The final A_List is transmitted to detection policy unit.

3.3. Detection Policy

Our proposed detection policy is also based on some rules. If sensor node's behavior violates some thresholds that are set during the normal execution of the sensor network than a particular flag is set against the respective field in the flag list (F_List).

The structure of F_List is shown in Table 2 and implementation of flag list is similar to that of A_List but it contains some flags in respective field positions. These are:

• N (miN): if value is less than the minimum threshold value and shows any attack pattern

• X (maX): if value is greater than the maximum threshold value and shows any attack pattern

• L (normaL): if value is between N and X or less/ greater than threshold value but does not show any attack pattern

Table 2. Flag List (F_List)

Node_ID	Packet Sent	Packet Received	Packet Forward	Packet Retransmit
X	N|X|L	N|X| L	N|X|L	N|X|L

A question arises that how the thresholds values are being set? These values may be set using any stochastic process that includes any intelligence. As far as sensor network is considered, we propose that these values should be set by executing the sensor network normally in a dummy environment that is similar to the actual sensor field.

In our case, there is a simulator that runs normally for certain number of times. It provides the audit lists of each simulation. These are used to set the threshold values in a threshold list (T_List) as shown in Table 3. T_List can be maintained by two ways. Firstly, there might be a unified threshold for all nodes. It means take the average of obtained values of all the nodes for each field. T_List contains single value for all the nodes in this type of implementation. Secondly, simulate the sensor network for n number of times. Calculate thresholds for each node by taking the averages of obtained values for each node of each field. This approach seems more realistic because it suits the dynamic nature of sensor network.

Table 3. Threshold List (T_List)

Node_ID	N_Snt	X_Snt	N_Rec	X_Rec	N_Fwd	X_Fwd	N_Rtm	X_Rtm
X	X_nSnt	X_xSnt	X_nRec	X_xRec	X_nFwd	X_xFwd	X_nRtm	X_xRtm

The following explanation explains the detection policy. There are two inputs A_List and T_List for this policy. These lists are analyzed to populate F_List.

4. Performance Evaluation

4.1. Simulation Environment

In our experiment, there are 100 audit lists; these are used to find minimum and maximum sending rates. These are placed in T_List.Once the Trace_List is populated, the A_List is formalized by counting the number of sends, receive, forward and retransmit for each node. Audit lists help in adjusting the threshold values in T_List.

4.2. Study of Sending Rate

During flood attack, the attacker sends more number of packets. Hence, the sending rate of the attacker nodes is increased by some fraction. There are 'nA' number of attackers that are randomly selected and their sending rates are increased.

Figure 1 provides sending rate analysis. It shows that attacker nodes are sending more number of packets than normal nodes.

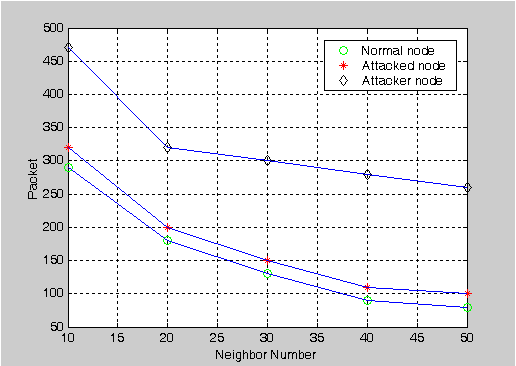

Figure 1. Study of Sending Rate

4.3. Study of Receiving Rate

In black-hole, sink-hole or worm-hole attack, the attacker receives more number of packets. Hence, the receiving rate of the attacker nodes is increased by some fraction. There are 'nA' numbers of attackers that are randomly selected and their receiving rates are increased.

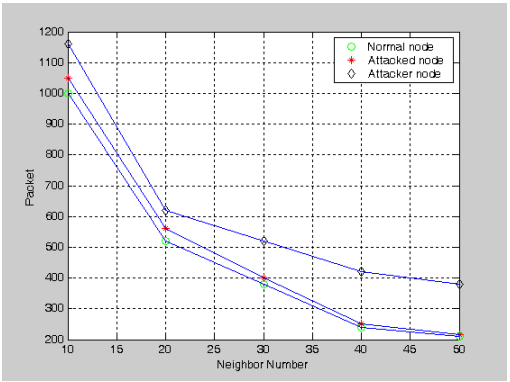

Figure 2. Study of Receiving Rate

Figure 2 provides receiving rate analysis. It shows that the attacker nodes are receiving more number of packets than normal nodes.

5. Conclusions

In this paper, an intrusion detection policy is proposed for securing wireless sensor networks from transport or routing layer attacks. The proposed intrusion detection policy achieves higher detection rate and receives high intrusion detection rate. They also guide that each node should be treated independently in WSNs, and purely

centralized detection schemes may fail to identify the network behavior whether it is normal or it is under any attack.

Acknowledgements

This work was supported by the Industrial Strategic Technology Development Program (10041740) funded by the Ministry of Knowledge Economy (MKE) Korea. It was also supported by the Natural Science Foundation of Jiangsu Province (No. BK2012461). Professor Jeong-Uk Kim is the corresponding author.

References

[1] Krontiris and T. Dimitriou, "Towards intrusion detection in wireless sensor networks", The 13th European Wireless Conference, **(2007)** April 1-4; Paris, France.
[2] A. H. Farooqi and F. A. Khan, "Intrusion Detection Systems for Wireless Sensor Networks: A Survey", Communications in Computer and Information Science, vol. 56, **(2009)**.
[3] Z. S. Bojkovic, B. M. Bakmaz and M. R. Bakmaz, "Security issues in wireless sensor networks", International Journal of Communications, vol. 2, no. 1, **(2008)**.
[4] I. F. Akyildiz, W. Su, Y. Sankarsubramaniam and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, vol. 40, no. 8, **(2002)**.
[5] R. Roman, J. Zhou and J. Lopez, "Applying Intrusion Detection Systems to wireless sensor networks", The 3rd IEEE Consumer Communications and Networking Conference, **(2006)** January 8-10; Las Vegas, USA.
[6] I. Krontiris, T. Dimitriou and T. Giannetsos, "LIDeA: A distributed lightweight intrusion detection architecture for sensor networks", Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, **(2008)** September 22-25; Istanbul, Turkey.
[7] A. H. Farooqi and F. A. Khan, "A survey of Intrusion Detection Systems for Wireless Sensor Networks", International Journal of Ad Hoc and Ubiquitous Computing, vol. 56, **(2009)**.
[8] A. P. R. Da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz and W. C. Wong, "Decentralized intrusion detection in wireless sensor networks", Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks, **(2005)** October 10-13; Montreal, Canada.
[9] M. S. Islam, R. H. Khan and D. M. Bappy, "A Hierarchical Intrusion Detection System in Wireless Sensor Networks", International Journal of Computer Science and Network Security, vol. 10, no. 8, **(2010)**.
[10] T. V. Phuong, L. X. Hung, S. J. Cho, Y. K. Lee and S. Lee, "An anomaly detection algorithm for detecting attacks in wireless sensor networks", Intelligence and Security Informatics, Lecture Notes in Computer Science, vol. 3975, **(2006)**.
[11] I. Krontiris, T. Dimitriou, T. Giannetsos and M. Mpasoukos, "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks", ALGOSENSORS'07 Proceedings of the 3rd International Conference on Algorithmic Aspects of Wireless Sensor Networks, **(2007)** July 14; Verlag Berlin, Germany.
[12] F. Liu, X. Cheng and D. Chen, "Insider Attacker Detection in Wireless Sensor Networks", Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM), **(2007)** May 6-12; Alaska, USA.
[13] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey", Elsevier Computer Networks, vol. 54, **(2010)**.

Author

Jiang Xu Jiang Xu received his bachelor and master degree from Nanjing University of Aeronautics and Astronautics (NUAA) China in 1997 and 2003 respectively. From 2003, he joined the School of Computer and Software at Nanjing University of Information Science and Technology as a lecturer. He is pursuing his Ph.D. degree in NUAA from 2010. His research interesting fields are data mining and database, wireless communication etc.