Dynamic Defense Strategy for Intrusion Detection in Wireless Sensor Networks†

Ponomarchuk Yulia*, Young Jin Nam**, Dae-Wha Seo*
*Dept. of Electronics and Computer Science, Kyungpook National University
**School of Computer & Information Technology, Daegu University
e-mail : rus_flash@hotmail.com

무선 센서 네트워크에서 침입 탐지를 위한 동적인 방어 기법†

뽀노마르추크 율리야*, 남영진**, 서대화*
*경북학교 전자전기컴퓨터학부, **대구대학교 컴퓨터 · IT 공학부

요 약

본 논문에서는 무선 센서 네트워크 상의 침입 탐지를 위한 동적인 방어 기법을 제안한다. 제안된 기법은 네트워크 상에 작은 수의 노드를 통하여 모니터링 작업을 수행하여 네트워크 상의 배터리 소모를 최소화함으로써 전체 네트워크의 라이프타임을 연장시킬 수 있도록 한다. 또한, 제안된 기법은 계층적 네트워크를 기반으로 한 간단한 구조를 갖고 있어, 센서 노드 내 배터리, 메모리, 컴퓨팅 파워 등의 제한된 자원에 효과적으로 대처할 수 있다.

1. 서론

Wireless sensor networks (WSN) are becoming an essential part of scientific, industrial and military projects. WSN usually consists of a large number of simple inexpensive wireless sensor nodes and one or several base stations (sink nodes) connecting the network to other networks or an end user. All sensors send results of measurements towards sink nodes in a hop-by-hop manner. Sensors have limited power, storage, processing resources and communication capabilities. Usually sensors have non-rechargeable batteries and left unattended after deployment.

WSNs are usually deployed in hazardous environment and are prone to natural disasters, inner failures, and attacks aimed to disrupt network's operation or modify transmitted data. For example, false alarms about chemical or biological threats of monitoring sensor network can cause an unfounded panic and neglect of warning systems. Therefore, a real attack on protected system can be preceded by DoS attack on a monitoring WSN. Sensor nodes are easily tampered, therefore, security of transmitted and stored data becomes an urgent question. Researchers pay a lot of attention to security issues in wireless networks, but due to strict resources constraints the most secure schemes can not be applied to WSNs directly. If an adversary uses a new assault, data encryption and integrity alone can not provide WSN's secure operation. Intrusion Detection System (IDS) can be interpreted as a second line of defense of the network. It can protect a WSN against unknown attacks and adapt itself to unpredicted changes in environment or network behavior.

This work is devoted to the design of a reliable IDS for WSNs regarding their specific features and limited resources of nodes, so that it could adapt itself to behavior of sensor nodes within the network.

2. 무선 센서 네트워크용 IDS 요구사항

WSNs inherit all peculiarities of wireless ad hoc and cellular networks except, first of all, mobility of nodes. WSNs have some specific features that make the design of IDS different. Every sensor node is totally independent from other nodes; it sends data towards a base station and receives control packets from it. Sensor nodes function in an unattended manner, but nodes of ad hoc networks are usually operated by a human user. Commonly the purpose of sensor networks is strictly specified before deployment, for example, to measure values of temperature. As a result, both hardware and software components are highly specialized in contrast to nodes of ad hoc networks. Power resources of a sensor node drain off very quickly, if it communicates with other nodes too actively. The batteries of nodes may be hard to recharge or not rechargeable, but in ad hoc networks a user of a node can take care of power supply. Moreover, a sensor node has very constrained resources of memory and processing power if compared to nodes of other wireless networks.

Sensor nodes are more susceptible to failures, harmful effects of the environment, or physical compromise than nodes of other networks. Therefore, any single node can not be trusted, as it may be easily tampered.

The deployment of sensor nodes commonly is more dense and random and their exact geographical position is unknown before deployment (and sometimes after it). On the contrary, a node of ad hoc or mobile networks can be supplied with a GPS receiver that will provide its exact geographical location.

†This research was supported by the Kyungpook National University BK21, MKE (Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute for Information Technology Advancement) (IITA-2008-C1090-0801-0045).

Due to mobility of nodes the traffic in ad hoc networks is quite random, but in sensor networks all messages are sent, as a rule, in a hop-by-hop manner towards a base station that is operated by a user or connects the WSN to another network. Usually paths for data transmissions are considered to be fixed within a given time interval [1-3].

According to the described above peculiarities of WSNs an IDS should satisfy the following conditions [2, 3].

1. Nodes of a network must not become more vulnerable with an IDS deployed, than they are without it.
2. To perform attack detection in a distributive manner data collection and analysis have to be done all over the network and alerts must be correlated.
3. Since only base stations can analyze audit data from the whole network, each node must be able to process only its own incoming and outcoming traffic and produce a reliable decision on the presence of an attack.
4. Each node must be capable of detecting and handling attacks from both an inside and outside adversary.
5. Each node must be able to accomplish these tasks utilizing its limited power, memory, and processing resources.

Also, an IDS must send alert messages to a base station to warn a user and refresh databases of anomalies and malicious neighbors within the whole network. It can be specialized to react to the specific threats to a WSN according to the application and utilize specific protocols used over it.

3. 관련 연구

In general, all IDSs for wireless networks can be divided into three classes according to the detection technique. *Signature-based* (or *misuse detection based*) IDS compares traffic features with predefined signatures of attacks or malicious actions. It allows detection of the majority of known attacks, but when an adversary launches a new type of assault a new signature should be created. Then this signature should be broadcast all over the network to update corresponding database on every node. *Anomaly-based* IDS checks the traffic on occurrence of any behavior different from the predefined or accepted normal patterns. It can detect novel attacks, but it has high false positive rate. *Specification-based* IDS, introduced by Brutch and Ko [4], uses a set of manually defined rules or constraints that are characteristic for an application running or correct protocol's operation. It seems to be the most suitable for WSNs, as the specification database requires less memory than others.

IDSs proposed by da Silva et al. [5] and Hai et al. [6] are based on a set of rules used for traffic analysis. This list includes:

1. *Interval rule:* an alert is raised if the delay between the arrivals of two consecutive messages is larger or smaller than the allowed limits.
2. *Integrity rule:* the message payload must be the same along the path from sender to receiver. This rule is discarded, if data aggregation is performed.
3. *Delay rule:* the retransmission of a message must occur within a specified time interval.
4. *Radio transmission range:* all messages must be received only from one of the neighbors.
5. *Jamming rule:* the number of collisions associated with a message must be lower than the expected number within the network.
6. *Repetition rule:* the same message can be retransmitted by the same neighbor only a limited number of times.
7. *Retransmission rule:* an alert is raised when a message is not forwarded as it should.

Hai et al. [6] considered only the first five rules. Above mentioned schemes assume that all nodes are provided with IDS agents, but only a number of them, monitoring nodes, have the agents active. If cluster-based routing protocol is used, the IDS can use the advantage of hierarchy as well by letting cluster heads (CHs) be monitoring nodes. However, these designs assume monitoring nodes to be trustworthy; there are no special recommendations how to resist a malicious monitoring node.

In general, intrusion detection algorithm consists of the following stages [5]. During *data acquisition phase* monitoring node listens to messages in promiscuous mode, filters, and stores important information. Stored information can include such message fields as source and destination nodes, next and previous hop nodes, message type, sequence number and data. In *rule application stage* parameters of a message are evaluated according to a sequence of rules specific for each type. If a message fails a rule, corresponding counter is incremented and the message is discarded. It is recommended to apply rules in order of increasing complexity. In the final stage – *intrusion detection phase* – an alert of the attack detection is broadcast if the value of failure counter is bigger than the corresponding threshold value, which is defined according to the network characteristics and can be changed during WSN lifetime.

Hai et al. [6] assumed that CHs transmit all their data directly to the base station. This proposition is quite unsound, as the majority of networks are too large and CHs transmit their data in a hop-by-hop manner that leads to the increase of network's vulnerabilities. If a located far away from base station CH is compromised, its attack is almost undetectable.

The design of IDS against node impersonation (Sybil attack) and DoS or resource depletion attacks, proposed by Onat and Miri [1], is based on node cooperation. Nodes know what to expect from their neighbors, can detect, and report anomalies to each other. All nodes implement intrusion detection that leads to higher power consumption. Nodes are stationary and no new node is deployed. Intrusion detection uses the average receive power and average packet arrival rate as features of neighbors' activities.

Ioannis et al. [3], designed an IDS to protect a WSN from selective forwarding attack and malicious modification. It is based on cooperative decision making and uses the rate at which packets are lost by neighbors as a source of analysis. Sender of a message is the collector of watchdogs' messages. If the majority of watchdogs detect an attack, then the suspected node is revoked and the base station is notified [3]. All watchdogs of a link should be within a communication range of each other.

The IDS, designed by Roman et al. [2], also uses local and global IDS agents preloaded on each node, but all alerts are sent to the base station that makes the decision. Local agent monitors packets which are addressed directly to it. Global agents are activated on CHs to monitor their neighbors' behavior in hierarchical architectures. In flat architectures spontaneous watchdogs technique is recommended, so that

only one global agent is activated per packet circulating in the network. Local and global agents of the same node cooperate as they use the same alert database. Nodes broadcast all changes to organize collaboration between each other. Attack detection alert is raised only by the base station after analysis of weighted reports from nodes.

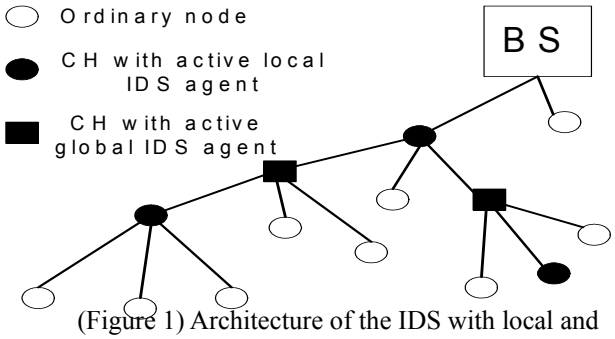
Techateerawat et al. [7] analyzed the distribution of monitoring nodes. Previously this question was not considered. Generally accepted opinion is either to allow monitoring functions to all nodes without exception, or to let CHs process network traffic. The first approach is not applicable to WSN due to high energy costs. The second one is also quite expensive and its security measures are redundant, as packet is checked at each intermediate node while transmitted. Techateerawat et al. [7], proposed three different strategies to select nodes detecting intrusion: 1) core defense – involves selecting IDS nodes around the central point (CH) to prevent intrusion into CH; 2) boundary defense – selects nodes at the perimeter of the cluster to protect it from outside intrusion; and 3) distributed defense – lies in voting algorithm of IDS agents activation. In each strategy, if an intrusion is detected, alarm messages are broadcast to activate IDS agents in neighboring nodes. So, intruder becomes encircled by nodes with active IDS agents and the network is protected from further attacks.

4. 제안된 IDS 구조

We assume that a WSN contains a large number of nodes divided into clusters, cluster heads are not fixed and change in a round-robin fashion to distribute the energy load evenly among the sensors in the network. The CHs are elected mainly according to the energy resources remained; they receive sensed information from ordinary sensors and transmit it to a base station in a hop-by-hop manner. There are several clustering protocols, for example, LEACH [8], PEGASIS [9], TEEN [10], APTEEN [11] that are generally recommended for use in wireless sensor networks. We assume that there is no data aggregation in the network.

As IDS should be distributed and cooperative for the needs of a WSN and regarding randomized rotation of CHs, IDS agents must be deployed in each sensor node, but activated only when needed to reduce power costs. Every node has two intrusion detection modules called local agent and global agent [2, 6, 12] (Fig. 1).

Local agent module is responsible for monitoring local information which is sent and received by the sensor (rules 1, 4, 5, 6). Any feature information is captured through the local data collection module and then passed on to the detection mechanism. It compares message fields' values to the predefined specifications. If the detection module finds signs of intrusion or misuse, then it responds on the local level and sends corresponding notification to the base station. When conclusion of the local agent is indecisive or cannot be derived from the local traffic, a global agent is activated to cooperate with other nodes and produce global response. Safe cooperation with other nodes requires secure communication.



(Figure 1) Architecture of the IDS with local and global agents

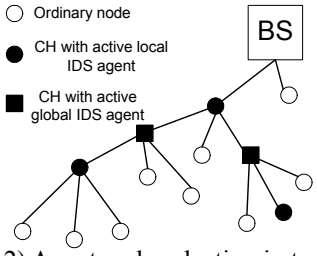
Both local and global agents use the same database of specifications and rules to detect anomalous behavior. All rules mentioned in the previous section can be used except retransmission rule, as it is included into delay rule. Application of thresholds may reduce the number of false alerts, for example, when packets are lost due to collisions within the network. Thresholds can be predefined according to empirical data, user's experience, expectations or common sense, or can be derived on the basis of statistics accumulated within the short interval of the network's safe functioning just after deployment when adversary is not able yet to initiate an attack. Given above rules prevent commonly considered attacks: jamming, DoS, malicious modification, spoofing, injection and modification of routing messages, replaying, selective forwarding, sinkhole and wormhole attack, Sybil attack, HELLO flooding, and acknowledgement spoofing [6, 13, 14].

The list of rules can be extended by adding specifications that are peculiar to the application executed in the network. For example, if the nodes sense temperature in some region and do not perform data encryption, then monitoring nodes can analyze the traffic in order to check if the temperature values belong to a certain reasonable interval. All rules can be further modified according to the changes in network traffic. In this case, the features of messages need to be stored in a buffer for further analysis. The larger is the buffer, the better is intrusion detection. Small buffer sizes lead to the high rate of false positives [3]. The problem is the choice of the size of such a buffer before network deployment for reliable anomaly detection and finding of a trade off between its size and nodes' memory constraints.

To perform intrusion detection and monitoring each node should store two more databases: the neighbor node database and malicious node database. The former contains 2 hop neighbors of a node with flags, whether they are CHs.

Our strategy utilizes the fact that ordinary nodes send their messages to CHs, which transmit data towards the base station organizing a tree-like hierarchy (Fig. 2). Then, ordinary nodes can be monitored by their CHs. Moreover, only local agents can be used for this task. Therefore, we propose that initially local IDS agents should be activated only on CHs to monitor incoming traffic from their cluster members and parental CHs. This type of topology is utilized to monitor CHs' behavior by global IDS agents as well. Global IDS agents can be activated only in a half of CHs (or even less). If a monitor detects an abnormal behavior of a node it increments the corresponding counter. If the counter value overcomes corresponding threshold, then alerts are sent to the neighbors of the suspect to activate their local IDS agents. So, suspected node will be surrounded by nodes with active IDS and will not be able to mount attacks undetected. If an IDS agent finds that the alert was unfounded it returns to the sleeping state and broadcasts the corresponding

message to its neighbors, so that the region remains guarded. Otherwise, a monitor sends attack detection message to the node-source of alert. If the majority of monitors detect an assault, then ID of the suspected node is included into malicious nodes database and corresponding messages are broadcast to the neighbors and the base station. Awakened IDS agents return to the sleeping state and cluster is reorganized if needed.



(Figure 2) Agent node selection in tree hierarchy

If an intruder compromises a node and initiates an attack, CH detects that, and all his messages are discarded. If he tampers a CH, then higher or lower level CH can detect an assault, activate global agent, and protect their segment of the network. In addition, ordinary nodes of the cluster are informed and activate their agents. If the attack is confirmed, then they reorganize the cluster. Even if an intruder compromises a segment of the network, this attack will be detected by higher level nodes and agents from neighboring "branches," as WSNs are usually dense and monitoring nodes can eavesdrop messages of all their neighbors.

The base station also analyzes the situation within the network, as encrypted alerts are sent to it.

<Table 1> Performance comparison of the proposed architecture

	IDS [5]	IDS [6]	IDS [1]	IDS [3]	IDS [2]	Proposed
Attacks	Sybil, wormhole, selective forwarding, DoS, replay, jamming, mal. modif., collisions	Selective forwarding, sinkhole, wormhole, HELLO flood, Sybil	Sybil, DoS	Blackhole, selective forwarding	Not specified	Sybil, wormhole, selective forwarding, DoS, replay, jamming, mal. modif., collisions
Features, if specified	Next & previous hops, type, origin, final dest., sequence #, data	Not specified	Average receive power, average packet arrival rate	Rate of message loosing	Received & sent message rate, data values	Next & previous hops, type, origin, final dest., sequence #, data
Class	Rules-based	Rules-based	Anomaly based	Specification-based	Anomaly-based	Rules- and specification-based
Architecture	Monitoring and ordinary nodes	Hierarchical, monitoring and ordinary nodes	All nodes are monitors	Based on watchdogs technique	Spontaneous watchdog technique	Monitoring and ordinary nodes

5. 결론 및 향후연구

The proposed IDS is based on specifications of a WSN behavior and sensed data range to reduce the amount of memory necessary for database storage. As well, it utilizes widely recommended rules for comparison of acquired data with statistics, derived from previous network (safe) functioning. It does not require activating IDS agents on all nodes. Only CHs have their local agents active to monitor incoming and outcoming traffic from their cluster members. Global agents need to be activated in each second CH, or even less often. The main goal of such an approach is to reduce power consumption for communication and constant surveillance of neighbors' behavior. When some indications of an attack are detected, a node sends alert messages to sensors, neighboring to the suspect, to activate their IDS agents and confirm or disprove an assault. In the former case ID of the suspect is included into malicious node data base and isolated, corresponding alert message is sent to the base station. In the latter one, IDS agents return to the sleeping state. The dynamic defense strategy allows an intruder to reach the first valid IDS agent and then it raises an alert broadcasting to strike back. We have not proved whether the proposed dynamic approach is more effective than common static defense strategy on actual WSN environments. Our future research will be devoted to the design of simulation and comparison of the two approaches.

참고문헌

[1] Onat I., Miri A. An Intrusion Detection System for Wireless Sensor Networks. IEEE Conf. WiMob'05, 2005.

[2] Roman R., Zhou J., Lopez J. Applying Intrusion Detection Systems to Wireless Sensor Networks. CCNC'06, 2006.

[3] Ioannis K., Dimitrou T., Freiling F.C. Towards Intrusion Detection in Wireless Sensor Networks. 13th European Wireless Conference, 2007.

[4] Brutch P., Ko C. Challenges in Intrusion Detection for Wireless Ad Hoc Networks. SAINT'03, 2003.

[5] Silva A.P., Martins M., Rocha B. Decentralized Intrusion Detection in Wireless Sensor Networks. Q2SWinet'05, 2005.

[6] Hai T.H., Khan F., Huh E.N. Hybrid Intrusion Detection System for Wireless Sensor Networks. ICCSA 2007, LNCS 4706, Part II, pp. 383-396, 2007.

[7] Techateerawat P., Jennings A. Energy Efficiency of Intrusion Detection Systems in Wireless Sensor Networks. Int. Conf. WI-IATW'06, 2006.

[8] Heinzelman W., Chandrakasan A., Balakrishnan H. Energy-Efficient Communication Protocol for Wireless Microsensor Networks. 33rd HICSS'00, 2000.

[9] Lindsey S., Raghavendra C. PEGASIS: Power-Efficient Gathering in Sensor Information Systems. IEEE Aerospace Conference, 2002.

[10] Manjeshwar A., Agrawal D.P. TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks. IPDPS'01, 2001.

[11] Manjeshwar A., Agrawal D.P. APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks. IPDPS 2002, 2002.

[12] Besemann C., Kawamura S., Rizzo F. Intrusion Detection System in Wireless Ad-Hoc Networks: Sybil Attack Detection and Others, 2003.

[13] Karlof C., Wagner D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. The 1st IEEE Int. Workshop on Sensor Network Protocols and Applications, 2003.

[14] Wang Y., Attebury G., Ramamurthy B. A Survey of Security Issues in Wireless Sensor Networks. IEEE Communications: Surveys, 2006.