A Survey of Encroachment Disclosure in Wireless Sensor Network

¹Sushma J. Gaurkar, ² Piyush k. Ingole

^{1,2} Dept of CSE ,G. H. Raisoni College of Engineering, Nagpur, India

Abstract

In wireless sensor network (WSN) security is the major issue because of its hostile nature. The traditional intrusion detection technique and traditional access control will not provide reliability and security if they do not work cooperatively. If the security is compromised, there could be serious consequences starting from theft of information, loss of privacy and reaching even bankruptcy of that institution. In this paper a brief survey on some recent intrusion detection technique & access control mechanism in wireless sensor network is presented and discusses them in detail.

Keywords: Wireless sensor network, intrusion detection technique, access control, security, decision tree.

1. Introduction

Wireless sensor network (WSN) refers to a system that consists of number of low-cost, resource limited sensor nodes to sense important data related to environment and to transmit it to sink node that provides. The WSN is in a hostile environment, where the deployers have no physical contact with the nodes, but attackers may. Usually, a wireless sensor network is deployed in a designated area without any fixed infrastructure where sensor nodes cooperate with each other to perform various applications. To save manufacturing cost, a sensor node is usually built as a small device, which has limited memory, a low-end processor, and is powered by a battery. Beside natural loss of sensor node it is also susceptible to various attacks. These attacks can not only disturb the normal working but also defeat the purpose of their deployment. An attacker can eavesdrop on all traffic, inject malicious packets, replay older messages, or compromise a sensor node.

There are various types of attacks like malicious, known and unknown etc describe in [10]. Generally, sensor nodes are most worried about two major security issues, which are privacy preserving and node authentication. A well-structured authentication mechanism can ensure that no unauthorized node is able to fraudulently participate and get sensitive information from WSNs.

As a result, several schemes have been proposed to secure communications in WSNs. When the data collected within a sensor network is valuable or should be kept confidential, then security measures should protect the access to this data. There are two main reasons why this is necessary. The first reason is concerned with the value of data. With the increasing connectivity of WSNs, environmental data will be available on demand almost everywhere in our environment from a surrounding WSN.

The second reason concerns the sensitivity of data. Hence, a security schemes which can deal with the attacks is very necessary for WSNs. Two complementary classes of approaches exist to protect WSNs, prevention-based approaches, such as access control, and detection-based approaches, such as intrusion detection (ID). In this paper, a survey on various intrusion detection system and access control mechanisms is conducted.

2. Literature Survey

Intrusion detection for WSN is an emerging field of research. This section represents the survey of various intrusion detection schemes.

2.1 Cluster based approach

A novel intrusion detection algorithm [2] provide an intrusion detection algorithm for wireless sensor networks which does not require prior knowledge of network behavior or a learning period in order to establish this knowledge. It takes more practical approach and applicable from small to middle size network like home and offices.

A cluster based sensor network is consider with N sensors uniformly distributed in clusters within the network area. The data aggregation is only done by the cluster head of each cluster. This approach operates with three neighborhood. The third neighborhood is a result of the data aggregation scheme, as it introduces the cluster as a separate neighborhood. In clustering method the base station has a complete overview over the network, prior to deployment. The algorithm used in this approach uses the anomaly detection technique in detection of intrusion and collects attribute vectors for each node in its neighborhood and comprises a data set consisting of all attribute vectors. The base station coordinates the clustering operation, and elects the cluster head of each cluster after the sensor nodes are deployed in the working environment. For the remaining network lifetime the election of new cluster heads are performed within the individual cluster based on remaining



reported energy level of nodes. New cluster heads are elected at a timely manner, when the current cluster head fails or if the current cluster head is found to be an insider attacker by the IDS. New nodes are not allowed into the clusters unless the base station explicitly organizes the introduction of the new node.

2.2 Reputation based intrusion detection system

In reputation based intrusion detection system [1] describe a model for IDS based on reputation and trust of the different nodes of a network for decision-making and analysis of possible sources of malicious attacks. It describe a hybrid approach which combines the hierarchical and the distributed approach. In this scheme the network is partitioned into several multi-hop clusters. Inside each cluster, and at the global level between cluster heads, the distributed architecture is used. The intrusion detections and assumptions, and the other IDS messages are exchanged inside a cluster, and the cluster members co-operatively take the decisions. By introducing a high co-operation between the nodes the drawbacks of the hierarchical architectures can be reduced.

2.3 Hybrid IDS

In HIDS [3] represents a novel hybrid IDS based on protocol analysis and decision making. In this, a HIDS is consider in a heterogeneous cluster based wireless sensor network. Cluster head is a one of sensor node in the cluster WSN but the capability of cluster head is better than other sensor node. The cluster head aggregates the sensed data from other sensor node in its own cluster. The HIDS consist of three model as shown in fig 1. It uses both misuse detection and anomaly detection technique. Both techniques filter the large number of packets records using anomaly detection model and further detection done with misuse detection model. Finally, the decision making model combines the outputs of anomaly detection and misuse detection models. It determines if an intrusion occurred, and classifies the type of attack found.

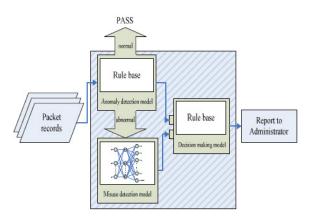


Figure 1: HIDS system architecture

2.3.1 Anomaly Detection Model

The anomaly detection model acts as a filter. It takes a large number of packet records first, and then sends abnormal packets for further detection with the misuse detection model, when the amount of information decreases. Because the anomaly detection uses a defined model of normal behavior, a packet is determined to be abnormal by the system when the current behavior varies from the model of normal behavior. It construct normal behavior profile for users and system activities, monitors the deviation of current event with respect to the established profile.

2.3.2 Misuse Detection Model

In misuse detection model, utilizes various models of well known attack behavior and built a model based on these behaviors. All abnormal packets, which were determined by the anomaly detection model, are subjected to the misuse detection model. Convert the abnormal packets into binary value in a preprocessing step, and input the misuse detection model to calculate the output and then deliver to the decision making model to integrate.

2.3.3 Decision Making Model

The decision making model is used to combine the outputs of the anomaly detection and misuse detection models. It determines whether or not an output is an intrusion, and the category of attack. It then has to report the results to the administrator to help them handle the state of the system and make further corrections. It uses rule-based method to establish the decision making model, using the rules to combine the outputs of two detection models.

The advantage of HIDS is that the cluster head is used to reduce energy consumption, amount of data in the entire network and to increase network lifetime but rules in the anomaly detection model are defined manually, so performance can not be verified through simulation.

2.3.4 Genetic algorithm based approach

In [5] represents a genetic algorithm with reduced complexity for intrusion detection of resource constrained multi-hop mobile sensor network. This scheme allocates the monitoring function to sensor nodes after evaluating its fitness based on integrity, residual battery power and coverage. Genetic algorithm are used to evaluate sensor node attributes by measuring the perceived threat and its suitability to host local monitoring node (LMN) that acts as trusted proxy agent for the sink and capable of securely monitoring its neighbors.

The security model used in this approach, the sink is considered a trusted component that establishes a

necessary trust relationship for secure forwarding of data between various node types. Nodes closest to the sink form the most trusted relationships. Farther nodes build the hierarchy of trust starting from the sink, which is apparent from the pre-determined routing decisions that are created during setup and later during re configuration. Ingredients of security architecture create a trust relationship between various node types for the reasons related command/message execution, data forwarding, etc. Any authentication is mediated through the sink and components of the trusted routing hierarchy.

A local monitoring mode is a trusted proxy agent for the sink. The sink allocates a CH to act as a LMN. In

case of a CH, it can use any of its member nodes as a pass through for monitoring purpose, which can increase the snoop coverage of the chosen cluster-head. selecting a cluster head as LMN, the sink sends the received signal strength (RSS) profile of its member nodes that are capable of listening to the monitored (suspicious) clusters. This data is used by the cluster head to select one of its members as a pass-through agent to monitor the cluster under observation.

One of the disadvantages is that as the network expanded, the generic algorithm convergence time increases exponentially.

2.3.5 Access Control

Security access is one of the key concerns for wireless sensor networks (WSNs). The secure authentication protocols of the most current security access schemes are complex. an access control mechanism should accomplish two tasks:

- Node authentication: Through authentication a deployed node proves its identity (ID) to its neighboring nodes and proves that it has the right to access the sensor network.
- 2) Key establishment: Shared keys should be established between a deployed node and its neighboring nodes to protect communications.

A preloaded public key certificate can be used to prove the identity of a new node. When the new node is deployed into the sensor network, its neighbors may verify the certificate to check whether the new node has a legitimate identity. By using this ID authentication, adversaries are prevented from directly deploying malicious nodes because they do not have corresponding certificates.

The access control mechanism describe in [9] based on Elliptic Curve Cryptography (ECC) for sensor networks. Different from conventional authentication methods based on the node identity, this access control protocol includes both the node identity and the node bootstrapping time into the authentication procedure. this access control mechanism provide authentication and also try to detect malicious node.

The authentication protocol and access control mechanism is designed based on security token and usage control (UCON) respectively describe in [4]. It has properties of attribute mutability and decision continuity. It provides authorization not only at the time of access also during its usage. In this three layer architecture is describe which includes base station layer, sink layer and sensor layer. The base station (BS) can act as an interface for WSNs to communicate with satellite, internet or mobile network.

A secure authentication protocol contains two steps: signature generation and signature authentication. The client node generates its own specific signature. The password is stored in both the memory of client node and the sever node. the signature provides a non repudiation property. This is true because only the client node herself can generate it. This scheme can perform access control with attribute mutability and decision continuity. In addition, the scheme can provide integrity and non-reputation properties. Also, it can resist against replay attack and DoS attack.

2.3.6 The trust based approach

The trust based approach [7] describes the dependency on the predictable behavior of nodes within communication distance with their continuous positive behavior. It uses the repeated game model to detect faulty (malicious) nodes through the cooperative effort in the sensor network and judges the trust of successive nodes.

In this approach each node maintains a rating of its successive node i.e. number of successful packet

transfers in the path. If the ratings of a node are above the threshold (expected minimum error rate), then the current node continues to transfer the packets. The current approach does not expect to calculate all ratings (packet transfer, noise, jamming, and infection factor) of its neighboring nodes and selects the path of highest ratings. Selecting the highest rating path requires additional processing time and is a burden on the energy budget in the sensor node and detects the malicious node using the trust factor. This approach is used to transfer the data securely and at the same time confirms the trust of next level node.

2.3.7 Disturbance based approach

In disturbance based [6] system describe a novel routing approach which attempts to detect situations which may produce the poor performance characteristic of an ongoing wormhole attack, by making nodes take account of disturbance (the impact of a forwarding commitment



on their peers), and diversify routes to attempt to find a wormhole-free path and reduce the influence of the attacker. A routing metric is built based upon static or dynamic disturbance characteristics of the local node.

In static disturbance The metric is static as it takes into account only the number of peers of the transmitting node. A peer is defined as any adjacent node with which the current node may interchange intelligible messages, negating those that merely interfere destructively. In the dynamic disturbance case, disturbance imposed is tracked using a cross-layer parameter, the shortest path activity factor.

The purpose behind this approach for wormhole detection is that without this avoidance, a functioning wormhole would draw in traffic leading to localized congestion, so a protocol which penalizes nodes in regions that would become busy under shortest path routing will draw new routes formed away from the wormhole. Dynamic disturbance refers to hypothetical disturbance that would occur if all application traffic was to be sent over shortest path routes.

Disturbance based routing schemes can provide a considerable improvement in wormhole avoidance over shortest path schemes, and that dynamic avoidance especially delivers major benefit in the active wormhole case. This scheme represents a distributed version of the statistical analysis of multipath (SAM) scheme, suitable as well for routing in multi-sink environments since each potential endpoint can take advantage of the network's collective estimates of wormhole locations.

3. Conclusion

This paper, represent a review of recent works on different approaches of IDS and access control for WSN. It has been observed that the intrusion detection system and access control mechanism will not provide proper security when they work separately. Therefore a combination of both of them is required to provide better security.

References

- "Reputation based intrusion detection system for wireless sensor network" by Gerrigagoitia, Keldor; Uribeetxeberria, Roberto; Zurutuza, Urko; Arenaza, Ignacio 2012 IEEE conference.
- [2] "A Novel Intrusion Detection Algorithm for Wireless Sensor networks" IEEE 2011 by Chun- ming Rong 1, Skjalg Eggen 2, Hong-bing Cheng.
- [3] "HIDS-DT: An Effective Hybrid Intrusion Detection System Based on Decision Tree" IEEE2010 BY Jie Yang1, Xin Chen1, Xudong Xiang1, Jianxiong Wan2.
- [4] "J. Wu and S. Shimamot, "Usage Control based Security Access Scheme for Wireless Sensor Networks," in the proc. IEEE International Conference on Communications(ICC 2010), May 2010.

- [5] R. Khanna, H. Liu and H. Chen, "Reduced Complexity Intrusion Detection in Sensor Networks Using Genetic Algorithm," in the proc. IEEE International Conference on Communications (ICC 2009), May 2009.
- [6] J. Harbin, P. Mitchell, D. Pearce, "Wireless Sensor Network Wormhole Avoidance Using Disturbance-Based Routing Schemes," in the proc. IEEE International Symposium on Wireless Communication Systems(ISWCS 2009), Sept. 2009. pp. 76-80.
- Sahota, Harleen Kaur, and Sandeep Singh Kang.
 "ZigBee: A Promising Wireless Technology." International Journal of Computer Science 1.
- [8] "A Trust-based Approach for Secure Packet Transfer in Wireless Sensor Networks" by Yenumula B. Reddy, Rastko R. Selmic International Journal on Advances in Security, vol 4 no 3 & 4, year 2011.
- [9] F. Pu, D. Sun, Q. Cao, H. Cai, F. Yang, "Pervasive Computing Context Access Control Based on UCONABC Model," in Proc. 2nd International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 06), Pasadena, California, USA, Dec. 2006, pp. 689–692.
- [10] Y. Zhou, Y. Zhang, and Y. Fang, "Access control in wireless sensor, networks," Ad Hoc Networks, vol. 5, no. 1, Jan. 2007, pp. 3-13.
- [11] C. Krauß, M. Schneider, C. Eckert, "On handling insider attacks in wireless sensor networks," Information Security Technical Report (ELSEVIER), vol. 13, no. 3, Aug. 2008, pp. 165-172.