Access Control And Intrusion Detection For Security In Wireless Sensor Network

Sushma J. Gaurkar, Piyush K.Ingole

Abstract: In wireless sensor networks (WSN), security access is one of the key component. Nodes in a wireless sensor network may be lost due to power exhaustion or malicious attacks. To prevent malicious nodes from joining the sensor network, access control is required in the design of sensor network protocols. WSN must be able to authorize and grant users the right to access to the network. On the other hand, WSN must organize data collected by sensors in such a way that an unauthorized entity cannot make arbitrary queries. The secure authentication protocol of traditional access control scheme do not provide concept of attribute mutability and can not perform continuous access decisions. The proposed work provide a new framework for low level intrusion detection at sensor with access control. This UCON scheme can perform access control with attribute mutability and decision continuity which provide more security. For the simulation purpose, . net framework is used.

Keywords: Access control, wireless sensor network, attribute mutability, Authentication, intrusion detection.

I. 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 sensor nodes, but attackers may. Attacks come in different sizes and shapes and can be conducted from the inside and the outside of the network. External attackers are attackers which are not legally part of the network. They could be part of another network which is linked to the target network using the same infrastructure or same communication technology. These nodes can carry out attacks without being authorized on the target network. These attackers may also be an outside node, which is not part of the network, but with jamming or passive eavesdropping capabilities. Internal attackers are compromised nodes which are authorized on the target network. These nodes can do more sophisticated attacks because they are seen as authorized by the network and fellow nodes. Ongoing attack can steer clear of traditional access control and intrusion detection components of WSN. Unknown attack always have quite different characteristics from usual attacks. Two complementary classes of approaches exist to protect WSN, prevention-based approaches such as access control and detection-based approaches, like intrusion detection. When access control and intrusion detection work separately then they may not produce higher security. The existing access control schemes only support identification and allow or deny access to protect network resources.

- Sushma J. Gaurkar, Department of Computer Science &Engineering, G.H. Raisoni College of Engineering, Nagpur, India sush.gaurkar@gmail.com
- Piyush K.Ingole, Department of Computer Science & Engineering, G.H. Raisoni College of Engineering, Nagpur, India piyush.ingole@gmail.com

However they do not support observing and reporting of the suspicious activities and modifying system protection as a result. It is assumed that access control should be based on a set of rules and intrusion detection should be based on different set of rules. However access control check the attributes of user or WSNs, which are also main operations of intrusion detection. Therefore the information needed by one component may be useful to another component.

A. UCON based access control

Access control is a important security service in Wireless sensor network, to prevent malicious nodes from joining the sensor network, access control is required. On one hand, WSN must be able to authorize and grant users the right to access to the network. On the other hand, WSN must organize data collected by sensors in such a way that an unauthorized entity (the adversary) cannot make arbitrary queries. This restricts the network access only to eligible users and sensor nodes, while queries from outsiders will not be answered or forwarded by nodes. the secure authentication protocols of the most current security access schemes have high expenses in calculation, storage and communication. Sensor nodes have limited processing capability, storage, and energy. Therefore, WSNs need authentication protocol with low expenses. Also there is no consideration of attribute mutability and decision continuity in the current scheme. The control over the data after the data are released from one entity to another is required. In all, WSN need a suitable access control model with distinguishing properties of attribute mutability and decision continuity. The proposed scheme uses UCON based access control mechanism[4] which is introduced as a next generation access control. Comparing with traditional access models, UCON has distinguishing properties of attribute mutability and decision continuity. These two kinds of properties can also providing ongoing observation to the user's behaviors and used in detecting ongoing attacks.

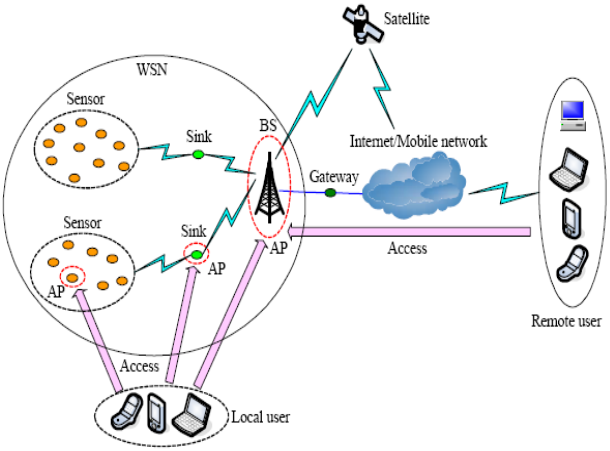

Fig 1: Access architecture of WSN

The proposed work use the three-layer wireless sensor network structure as clustered sensor network, 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. As illustrated in Fig. 1, BS, sink and sensor are the access points (AP) when users access the data in the WSN. Local users access the WSN directly. However, remote users need access the WSN through satellite, Internet or mobile network.

B. Intrusion detection

Intrusion detection poses many challenges to WSNs, mainly due to the lack of resources. Besides, methods developed to be used in traditional networks cannot be applied directly to WSNs, since they demand resources not available in sensor networks. WSNs are typically application oriented, which means they are designed to have very specific characteristics according to the target application. The intrusion detection assumes that the normal system behavior is different from the behavior of a system under attack. The several possible WSN configurations make difficult the definition of the “usual” or “expected” system behavior. The proposed scheme uses decision tree (DT) which is concept of data mining technique. Decision tree is effective method for solving machine learning problems. A decision tree is learned and reasoned from the feature-based examples by heuristic information.

II. Related Work

Intrusion detection for WSN is an emerging field of research . 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. 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. Sahni ,J Kaur, S Sharma in [13] describe security issues and solusions in WSN. It describe threat types and its detection based on net.work topology layer analysis 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. R. Khanna describe a genetic algorithm [5]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 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. 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.

III. Proposed Methodology

From the literature survey and analysis of network it is observed that data security is a big issue in WSN. Access control and Intrusion detection is of great importance in WSN because important data is stored in sensor node and also because of hostile environment. Proposed system uses the concept of UCON based access control and decision tree method to detect known and unknown intrusion for higher security. Proposed work is in two phases:

- UCON based reference monitor process for access control
- Intrusion detection process in sensor

A. UCON based reference monitor process for access control

The usage control (UCON) model is introduced as a next generation access control model. UCON extends traditional access control to consider the problem of authorization not only at the time of access to a resource but also during its usage. The UCON model consist of eight components: subjects ,subjects attributes, object, object attributes, rights, authorization, obligations, and conditions [8]. The most important properties that distinguish UCON from traditional access control model are the continuity of usage decisions and the mutability of attributes [11. Fig 1.shows the relationship between traditional access control and usage control.

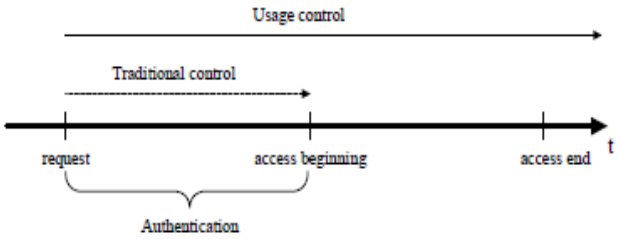

Fig 2: Usage control definition

One of the most critical issues in using UCON for enforcing access into WSNs is to use the concept of reference monitor(RM). ISO has published ISO/IEC 10181-3 standard [12] for access control framework by using reference monitor.

B. Intrusion detection process in sensor

The proposed work focuses on known and unknown attacks. Due to lack of physical protection , sensor nodes are usually vulnerable to strong attacks. Every node of WSN can perform usage control and intrusion detection. The rule of these two component are in the same rule pool. As the sensor node are resource constraint the intrusion detection done in two level: (1) high level intrusion detection and (2) low level intrusion detection at sensor. The proposed work focuses on low level intrusion detection performed at sensor. In order to perform intrusion detection ,the proposed work uses decision tree (DT) as a classifier for analyzing data. The decision tree act as classifier to verify the characteristic data of users behavior. There are three criteria for constructing a decision tree: the information gain, the gain ratio and the Gini index. There are three steps to design decision tree based intrusion detection. The first step is defining and initializing variables that will be used in the ensuing process. The second step is defining a set of primary detection rules. A detection rule contains a set of keywords that must be checked to trigger an alarm. And finally, the third step is defining a set of primary action rules that describe the behavior after analyzing the attribute data.

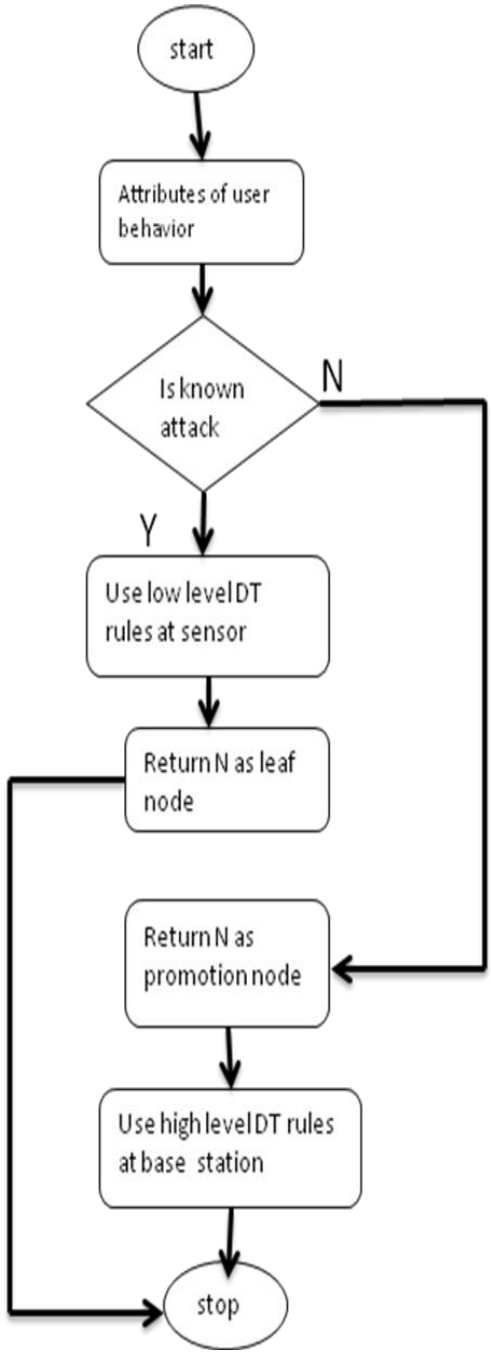

Fig 3: Intrusion detection model

Low level DT construction in sensor:

The DT construction scheme for sensor must have low complexity because the resources of sensors are limited. The DT in our scheme contains three types of nodes: ordinary, leaf and promotion nodes. Each node is represented by *N* (*A, D, M*) where *A* is an attribute set, *D* is a set of detection rules and *C* is a set of countermeasure. The attribute set *A* denotes the set of attributes which is already used to decompose the tree and *D* is the set of detection rules that are matched at that

node. The initial root node contains the complete set of detection rules, an empty set of attributes and an empty set of matched rules. After that, decompose each node according to the set of possible attributes using the appropriate inference rules. Leaves are nodes that cannot be transformed anymore.

They can be used to report attacks because of detection rules contained in their last field. A promotion node is a node at which can be further processed by the sink as a root node of subtree. Here some definitions and notations are given which used in DT construction.

Definition 1: Let *T* be a set of criterion variable and *d* be a rule which is the dimension of *T*. We define the function *Drawn*(*d*)={*v*1,*v*2,…,*vk*}.

The function can be extended to a set of rules *L* by:

$$Drawn(D) = \bigcup_{d \in D} Drawn(d)$$

Definition 2: function *Obtain*(*N*(*F*, *D*, *M*)) as a subtree. This function send *N*(*F*, *D*, *M*) to a sink. Then *N*(*F*, *D*, *M*) can be further processed by the sink and a subtree will be returned to the sensor. The root node of the subtree is *N*(*F*, *D*, *M*), so that the subtree can be integrated with the current tree in the sensor. The function *Drawn* is used to extract the parameters of the local low level rules. Also, the function *Obtain used* to get a subtree from the sink. In other words if the sensor can not deal with some situations, the sink can help to decompose the current node *N* into a subtree base on high level rules.

The process of low level tree construction is as follows:

Step 1: Start from an initial node N

Step 2: Analyse the feature set F and the rules set D of the current node.

Step 3: check attribute A with set of rules If yes then return N as leaf node otherwise call obtain(N) function to get a subtree & send it as promotion to base station.

Step 4: scan all remainder node of the current parent tree .

C. Simulation

In this section, we mainly use simulations to analyze and evaluate the performance of the proposed methodology. Simulation experiment is carried out in dot net.

A. Simulation Setup

Simulation setup parameters of the model are mentioned in Table 1.

Table 1: Transmission Parameters Value

No. of Nodes	50
Area Size	200X 200 sq.m
Queue Limit/ Type	Droptail/100
MAC Type	802.15.4
Transmission Range	15m
Simulation Time	50s
Packet Type/size	CBR/512 bytes
Data Rate	100 KBPS
Initial Energy	5 Joules

B. Simulation and analysis

Fifty sensor nodes and one base station are placed randomly in 200 X 200 square meters area. Topology is different from the existing TSP. 512byte packets are used. Each node has their initial energy of 5 joule. Figure 4 indicates the WSN used for simulation.

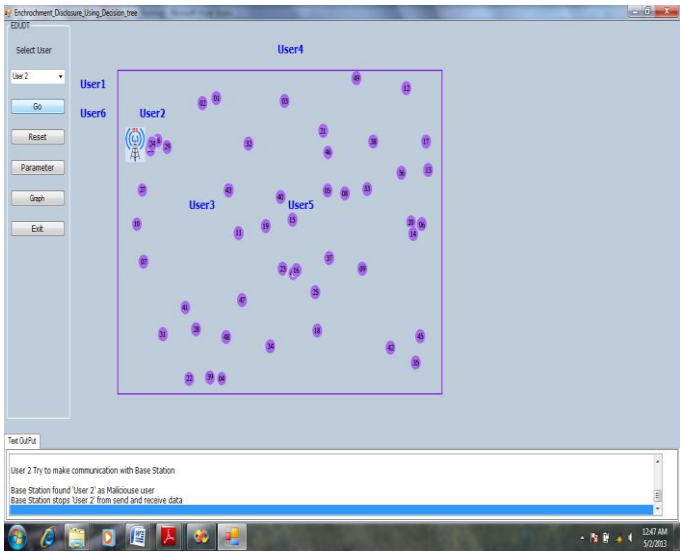

Fig 4: WSN used for Simulation

D. Conclusion and Future work

The proposed work provide a new framework for security scheme to integrate access control and intrusion detection in WSNs. It include low level intrusion detection with decision tree at sensor for known attack detection. In future work, we will explore high level decision tree construction in base station and detection of unknown attack.

References

[1]. "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.*

[7]. "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.*

[8]. 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.

[9]. 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.*

[10]. 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.

[11]. X. Zhang, F. P. Presicce, and R. Sandhu, "Formal Model and Policy Specification of Usage Control," *ACM Transactions on Information and System Security*, vol. 8, no. 4, Nov. 2005, pp. 351–387.

[12]. *Security frameworks for open systems: Access control framework*, ISO/IEC Standard 10181-3, 1996.

[13]. Varsha Sahni ,Jaspreet Kaur, Sonia Sharma "Security issues and solution in wireless sensor network " (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (2) , 2012,3295-3304