Cross Layer Based Anomaly Intrusion Detection In Wireless Sensor Network

1V. Srinivasan and 2M. Vidhya

1Professor and Head, Dept of CSE, Annamalai University, Chidambaram, Tamil Nadu, India.
2PG Student, Dept of CSE, Annamalai University, Chidambaram, Tamil Nadu, India.

ABSTRACT

The wireless sensor networks (WSN) are especially vulnerable to diverse attacks at dissimilar layers of the protocol stack in OSI model. Earlier, Intrusion detection system is only used to identify an intrusion at the network layer without identifying at the MAC and physical layer, so it’s make these systems less effectiveness. In this paper we propose a pioneer intrusion detection system depends on cross layer interface among the network, MAC and physical layers. The main objective is to develop single intrusion detection system that works on dissimilar layers of the OSI model and to identify dissimilar types of attacks on various layers of the OSI model.

INTRODUCTION

Wireless Sensor Networks (WSNs) have been collected of sensor nodes and sinks. Sensor nodes are having the power of self-healing and self-organizing. They have been decentralized and distributed in environment where information transmitted through multi hop intermediate nodes. The basic objective of a sensor node is to gather information from its surrounding atmosphere and convey to the sink. WSNs have several applications and are used in situation such as detecting changed climate, monitoring atmosphere and environment, and various other surveillance and military applications. Regularly sensor nodes are deployed in areas where wired connections are not possible. WSNs are implemented in physical cruel and intimidating situation where nodes are always exposed to physical security risks damages. Moreover, self-organizing nature, low battery power supply, limited bandwidth support, distributed operations using open wireless medium, multi hop traffic forwarding, and dependency on other nodes are such characteristics of sensor networks that expose it to many security attacks at all layers of the OSI model (Padmavathi, G. and D. Shanmugapriya, 2009). Many security-related solutions for WSNs have been proposed such as authentication, key exchange (Camtepe, S. and B. Yener, 2005), and secure routing or security mechanisms (Dimitriou, T. and I. Krontiris, 2006; Ganeriwal, S., and D. Estrin, 2005) for precise attacks. These security mechanisms are capable of ensuring security at some level; however they cannot eliminate most of the security attacks. An Intrusion Detection System (IDS) is one possible answer to address a wide range of security attacks in WSNs.

1. Related work:

In this section, we are going to discuss existing techniques i.e. Anomaly-based IDSs can detect novel attack still they are generating more false alarm. Signature-based IDSs can detect well known attack but couldn’t detect novel attack. Hybrid IDS is combination of both anomaly and signature based IDS so it can detect new and existing attack but it required more resources and computation power.

Da Silva (2005) and Onat et al. (2005) proposed IDS examining nodes listen to messages in their radio range and use a buffer to store precise message fields that might be helpful to an IDS system running within a sensor node, but no details are given concerning how this systems are works. In these architectures, there is no collaboration among the monitor nodes. Both papers lead to conclude that the buffer size is an main factor that greatly affects the rate of false alarms.

Loo et al. (2006) and Bhuse and Gupta (2006) described IDS for routing attacks in sensor network. They have been assumed in both papers that routing protocols for ad hoc networks can be applied to WSNs. A clustering algorithm is used to build a model of usual traffic behavior. Abnormal traffic is detected and also

Corresponding Author: V. Srinivasan, Professor and Head, Dept of CSE, Annamalai University, Chidambaram, Tamil Nadu, India, E-mail: vscseau@gmail.com.
hidden attacks are detected using this approach. The main advantages are power consumption significantly reduced and a wide range of routing attack can be detected. The disadvantage is no collaboration exists with other neighbor nodes.

Edith C.H. Ngai et al. (2006) proposed Sinkhole attacks can be detected via the algorithm. The first phase consists of finding a list of suspected nodes via estimating the attacked area. The second phase, the intruder would be identified via analyzing the routing pattern in the affected area. In detail, a request message containing the IDs of all affected nodes is broadcasted by base station. A timestamp is included in a request signed with the private key of the base station to prevent replay attacks. The affected node replies with its own ID the ID of the next-hop node and the routing cost (e.g. hop-count) to that node on receiving the request (Ayyasamy, A. and K. Venkatachalapathy, 2013). The reply message is sent along the reverse path in the broadcast, as the next-hop and routing cost could already be affected by the attack. At the base station, constructing a tree using the next-hop information allows to analyze the routing pattern. In a sinkhole attack, all network traffic flow towards the same destination which reveals the identity of the intruder.

Krontiris et al. (2007) design IDS to detect the black hole and the selective forwarding attack. In order to detect the attacker, every node monitors its neighborhood and collaborates with its nearest neighbors (Ayyasamy, A. and K. Venkatachalapathy, 2012). They can detect deviations from normal behavior by following a rule-based approach the attacker node is identified, if more than half of the watchdog nodes raise an alert for this node. This approach is extended in (Ioannis Krontiris, 2008), in order to detect sinkhole attacks.

2. Methodology:
In this section, present proposed work of cross layer intrusion detection system. The function of intrusion detection system is to detect intruders while they try to communicate with the network node and the function of cross layer IDS could be detect multi layer attacks. The proposed work can be divided into four modules. Fig. 1 shows the details of block diagram of proposed work.

2.1 Network organization.
2.2 Cross Layer Intrusion Detection Agent (CLIDA) Architecture.
2.3 Intrusion detection layers.
2.4 self healing module.

Fig. 1: Block diagram of proposed work.

2.1 Network Organization:
WSNs have been emerged as a novel information collecting system based on the collaborative efforts with limited resource of large number of tiny sensors. Fig. 2 shows the network organization and these details are illustrate in sections 2.1.1, 2.1.2 and 2.1.3.

Fig. 2: Network organization.

2.1.1 Chain Cluster Topology:
Let us take cluster-based network topology. This topology can be divide the network into many clusters and choose the cluster head (CH) node which has been the greatest energy reserves in the clusters (Su, C.C., 2005). A novel network self-organization approach, which integrates cluster-based and chain based approaches. This novel approach is called chains clustering topology.

2.1.2 HEEP Protocol:
Hybrid Energy Efficiency Protocol (HEEP) has been presented in (Boubiche, D., A. Bilami, 2011). It consists at each cluster to be establishing a chain of neighborhood nodes. The base station takes the responsibility of forming the clusters, choosing the clusters and establishment of chains of node depends on
routing information sent by all networks then all the network nodes will broadcast gathered information to their Cluster Head (CH) via the chain of neighboring nodes. Then CHs will be take the responsibility of transmitting received information directly to the Base Station (BS), or indirectly via the neighboring CHs. HEEP uses are random rotation of the CH roles, which controls energy dissipation and prevents that the nodes chosen as CHs don’t rapidly die. HEEP has two important stages which are initialization and transmission stages. The initialization stage forms chained clusters and elects CHs and the transmission stage where collected data’s are transmitted.

2.1.3 SMAC Protocol:
SMAC is a sensor medium-access control protocol designed for wireless sensor networks. For access the medium, we used the SMAC protocol (Ye John Heidemann, 2002). The idle listening, nodes must periodically sleep to reduce energy consumption. During transmission of other nodes the SMAC sets the radio to sleep. It’s uses in-channel signaling. SMAC can applies message passing to reduce contention latency for sensor-network applications and let us take the use of RTS / CTS (Wei Ye, 2004) mechanism in the process of data transmission. A Pair wise Key Pre distribution Scheme (Du, W., 2005) for Wireless Sensor Networks based on symmetric keys is assumed. By this approach key information’s are distributed to all sensor nodes to prior deployment.

2.2 CLIDA Architecture:
CLIDA is the entity via which the layers and applications communicate. It’s including two parts which are interaction interface and cross-layer data module. Fig. 3 shows the CLIDA Architecture and these details are illustrate in sections 2.2.1 and 2.2.2.

![Fig. 3: Architecture of CLIDA.](image)

2.2.1 Interaction interface.
Interaction interface is making easy the communication between the layers and their functions on the one side and the CLIDA agent on the other side. Its main objective is the management of sub-interfaces which provide access to the layers. Every sub interface describes technique for reading and writing to ease the management of limits of the related protocol. Through these techniques have been made the collection and / or updating data i.e. calculated RSSI, routing tables, etc.

2.2.2 Cross-layer data module:
The Cross-layer data module corresponds to data to make them rapidly accessible by all layer protocols. This module provided data’s are the origin of any Cross-layer adaptation and optimization and also maintaining up to date data via Cross layer interaction interfaces.

2.3 Intrusion Detection Layers:
The architecture of cross layer that utilizes communication and collaboration of three neighboring layers in the OSI model i.e. network, Mac and physical layers is proposed. Fig.4 shows the flow chart of intrusion detection at each layer and these details are illustrate in sections 2.3.1, 2.3.2 and 2.3.3.

2.3.1 Network Layer:
Verify the existence of the transmitting node in the routing table. A routing table includes the information essential in forwarding a packet along the best path toward its destination. Every packet contains information about its source and destination. After receiving the packet, the network device studies the packet completely and compares it to the routing table entry for providing the best match to its destination. Routing is the process of selecting best paths in a network. The eq. (1) represented as metric value.

\[ M = x_1 \times H + (x_2 \times \text{stability} + x_3 \times \text{load})/H. \]  

(1)

Where, \( x_1, x_2, x_3 \): weights of hop number, stability, traffic load
H: hop number
Stability=0.1* node+ Packet Count
Load=queue/total buffer

**Fig. 4:** Flow chart of intrusion detection layers.

### 2.3.2 MAC Layer:
While utilizing the routing information at the MAC layer, every sensor node can formerly know the origin of packets that will be received. By this, any node attempt to communicate with the sensor nodes are instantly detected as an intruder if it is not included in the routing path. The every point-to-point link is technically a hop. A hop is one segment of the path between origin and destination. Hop occurring every time packets are passed to the next device.
- Routing information uses hop count as the metric.
- Hop Count = Number of Routers data from source to destination.

### 2.3.3 Physical Layer:
Received RTS packets of the intruder’s node by the targeted node, intrusion detection system verify if it is one of the neighbors in the routing path by consulting the routing table at the network layer and also authenticity of the intruder node will be verified by measuring the Received Signal Strength Indicator (RSSI) of the received packet. RSSI represents the entire received power. The received power \( P_r \) is represented as in eq. (2)

\[
P_r = P_t \cdot \left( \frac{1}{d} \right)^n
\]

Here, \( P_r \) - receiving power, \( P_t \) - transmitted power, \( d \) - Distance between sender and receiver node
\( n \) - Transmission factor whose value depends on the propagation environment

### 2.4 Self Healing Module:
Self healing module is proposed [19] for fixing the intrusion attacks during the transaction in wireless sensor networks [Fig. 5]. An intrusion detection system recognizing the attacks efficiently but it couldn’t able to do any fixing action. In later than IDS, self healing model able to fixing the network by using self healing algorithm. Fig. 6 shows the details of the work flow of self healing algorithm.

**Fig. 5:** Self healing module.

**Fig. 6:** Flow chart of self healing module.
RESULT AND DISCUSSION

Analysis of intrusion detection is executed by using the network simulator NS2. In this execution, our simulated model is built on 50 nodes distributed randomly on a square surface. Initially we calculated the number of intruder nodes detected during simulation progresses. Let us assume that attacker nodes target and attack randomly network nodes after being in passive state and then send RTS packet to each tow frame time. The Fig. 7 shows that result.

![Fig. 7: Number of detected intruder nodes v/s simulation time.](image)

Secondly, the estimated step is to analyze the behavior of IDS. For this, we measured the total no. of delivered message by the base station entire the simulation period. All intruder nodes attempt to make their attacks in random periods. In our simulation, the intruder nodes which are closest to the CHs attempt to create a sinkhole i.e. to lure traffic a compromised node while other intruder nodes (distant from CHs) can be perform operation of other attacks. Fig. 8 shows the result. With our IDS can prevent the major attack that affects the data routing at the network layer.

![Fig. 8: Total no. of delivered message to BS v/s simulation time.](image)

Thirdly, the performance of our IDS against the attacks at the MAC layer is evaluated. The intruder node can perform attacks of exhausting of more energy and to measure total energy reserves of the network nodes to the entire simulation period. Fig.9 shows the results:

![Fig. 9: Total energy reserves v/s simulation time.](image)

**Performance Evaluation:**

The possibility of detection of an intruder, \( P_{\text{det}} \), based on two aspects: no. of attacked nodes in a cluster and likelihood of a missed detection of an attacked node. The number of nodes attacked is given as \( Z \). In the proposed method the intruder nodes are not only detected if the compromised nodes don’t accept any packet from the malicious node. Then the likelihood of a missed detection is equivalent to the likelihood of a collision occurring in a transmission link \( P_{\text{col}} \).

Binomial rule in eq. (3)
By using the Binomial rule we can define the possibility of detection of an intruder as in eq. (4)

\[ P_{\text{det}} = \left( \frac{Z}{1} \right) (1 - P_{\text{det}})^{Z_i} \]

Basing on equation 4 we can calculate the possibility of detecting M intruder in the network in eq. (5)

\[ P_{\text{det}} = \left( \frac{Z}{M} \right) (1 - P_{\text{det}})^{M} \]

The whole network can identify the attackers and the possibility of detecting augments gradually with the expansion of the number of attacked nodes and the declining of collusion amount. Let us consider the attacker node attacks all nodes within its communication range. Then the average number of attacked node by an intruder can be equal to eq. (6)

\[ Z = (N - 1) \pi r^2/v \]

Where: \( v \) is the area of the range region, \( N \) is the number of nodes in that region and \( r \) is the intruder transmission radius.

The proposed IDS are energy efficient. To approximate the total energy consumed by our IDS, for that calculate the consumed energy of IDS on each attacked node in eq. (7)

\[ E_{\text{C}} + E_{\text{p}} + E_{\text{sx}} \]

Where: \( E_{\text{C}} \) is the energy consumed to detect the intrusion on node \( i \), \( E_{\text{p}} \) is receiving of packet from intruder, \( E_{\text{p}} \) is the processing of intruder detection and \( E_{\text{sx}} \) is the sending the alarm message. Then the total energy consumed by our IDS to defend the network from M attacker (j) nodes is equal to eq. (8)

\[ \text{Energy}_{\text{IDS}} = \sum_{j=0}^{M} \sum_{i=0}^{Z_j} E_{\text{Ri}} \]

We can reduce the unnecessary active node which helps us to reduce the energy consumption. Fig.10 shows the result.

**Fig. 10**: Energy Consumption v/s the % of detected intruder.

4. **Conclusion**:  
While designing a security mechanism, we should consider the some degrees of resources of WSNs. Anomaly-based IDSs are trivial in nature; still they are generating more fake alarm. Signature-based IDSs are appropriate for comparatively large-sized WSNs; still they have some expenses such as updating and inserting new signatures. Our main objective is security, so our proposed cross layer intrusion detection system dedicated for wireless sensor networks. Our approach is to develop single cross layer intrusion detection system that operates on dissimilar layers of the OSI model and to identify dissimilar types of attacks on various layers of the OSI model. The simulation results demonstrate the performance provided by our IDS in terms of detecting and preventing the various intrusion attacks.

**REFERENCES**

