IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 14, Issue 1 (Sep. - Oct. 2013), PP 61-70
www.iosrjournals.org

Distributed Intrusion Detection System for Wireless Sensor Networks

Aravendra Kumar Sharma[1],Sushil Kumar Saroj[2], Prashant Kumar[3]
[1](School *of Computer ScienceEngineeringGalgotia's University, Greater Noida, India)*
[2]*(Computer Science and Engineering Department, Galgotias College, Greater Noida, India)*
[3](School *of Computer Science EngineeringGalgotia'sUniversity, Greater Noida, India)*

Abstract: *Wireless sensor networks are exposed to different types of security threats that can reduce the performance of the whole network; that might result in serious problems like denial of service attacks, routing attacks, Sybil attack etc. Defensive mechanisms like Key management protocols, authentication protocols and secure routing cannot provide security to WSNs for these types of attacks. Intrusion detection system is a solution to this problem. It analyses the network by collecting sufficient amount of data and detects anomalous behaviour of sensor node. IDS based security mechanisms suggested for other network models such as ad hoc networks, cannot directly be used in WSNs. Researchers have proposed various intrusion detection systems for wireless sensor networks during the last few years. Essentially these approaches can be classified into two main categories i.e. distributed and stand alone. Distributed IDS can be further classified into hierarchical, mobile agent based and hybrid IDS. This paper presents distributed intrusion detection system for wireless sensor networks.*

Keywords: *Wireless Sensor Networks, Security, Intrusion Detection System*

I. INTRODUCTION

Wireless sensor networks are the combinations of tiny sensors which communicate with each other using wireless communication.A wireless sensor network (WSN) is a highly distributed network of resource-constrained and wireless devices called sensor nodes. Each sensor node monitors some physical phenomenon (e.g., humidity, temperature, pressure, light) inside the area of deployment. The collected measurementsare sent to a base station. The communication range ofsensor nodes is limited to tens of meters and hence notall of them can directly communicate with the base station.Therefore, data are sent hop-by-hop from one sensor nodeto another until they reach the base station. [1]

Most of the applications in WSNs require the unattended operation of a large number of sensor nodes. Thisraises immediate problems for administration and utilization.Even worse; sometimes it is not possible to approach thedeployment area at all, like for example in hostile, dangerousenvironments or military applications. So, sensor networksneed to become autonomous and exhibit responsiveness andadaptability to evolution changesin real time, without explicituser or administrator action.

Some basic features of sensor networks are:
– Self-organization
– Short-range broadcast communication and multi-hop routing
– Dense deployment and cooperative sensors
– Frequently changing topology, due to fading and node failures
– Limitations in computational resources, such as energy and memory[2]

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems .They are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use them for other purposes, such as identifying problems with security policies, documenting existing threats, and preventing individuals from violating security policies. Intrusion Detection System is an alarm system,which attempts to detect the intrusion against a system ornetwork. It includesdata collection, feature extraction, behavior classification, reporting andresponse.

IDS architectures are classified into two basic categories: host-based and network-based, depending on the data collection mechanism. Host-based IDS consult several types of log files (kernel, system, application, etc.) and compare the logs against an internal database of common signatures for known attacks. Network-based

IDS operate differently from host-based IDS. The design philosophy of a network based IDS are to scan network packets, auditing packet information, and logging any suspicious packets. Additionally, IDS architectures can further be classified based on the detection technique. Signature based IDS centers on finding an occurrence of predefined signatures or behavior that matches a previously known malicious action or indicates an intrusion. Anomaly-based IDS check for any behavior that fall outside the predefined or accepted model of behavior. In another type ofIntrusion detection has been introduced. Specification based IDSdefines a protocol or aprogram's correct operations. Intrusion is indicatedaccording to those constraints. This typeof IDS may detect unknown attacks, while showing low false positive rate.

II. Security Issues in Wireless Sensor Networks

Security is WSNs is quite different from traditional network security mechanisms. This is because of two major reasons. Firstly, there are severe constraints on these devices namely their minimal energy, computational and communicational capabilities. Secondly, there is an additional risk of physical attacks such as node capture and tampering.

2.1 Security Requirements

The goal of security services in WSNs is to protect the information and resources from attacks and misbehaviour. The security requirements in WSNs include:

1. Availability, which ensures that the desired network services are available even in the presence of denial-of-service attacks
2. Authorization, which ensures that only authorized sensors can be involved in providing information to network services
3. Authentication, which ensures that the communicationfrom one node to another node is genuine, that is, amalicious node cannot masquerade as a trusted networknode
4. Confidentiality, which ensures that a given message cannotbe understood by anyone other than the desiredrecipients
5. Integrity, which ensures that a message sent from onenode to another is not modified by malicious intermediatenodes

Non-repudiation, which denotes that a node cannot denysending a message it has previously sentFreshness, which implies that the data is recent andensures that no adversary can replay old messages.

Moreover, as new sensors are deployed and old sensorsfail, we suggest that forward and backward secrecy should alsobe considered:

1. Forward secrecy: a sensor should not be able to read anyfuture messages after it leaves the network.
2. Backward secrecy: a joining sensor should not be able to read any previously transmitted message.[3]

2.2 Threats in WSN

The inherent characteristics of wireless sensor networks make them especially prone to attacks. As data is transmitted over the air, it is extremely easy for an adversary to sniff traffic. A layer based classification of attacks is shown in Figure 2.1 and classification on the basis of attack characteristics is shown in Figure 2.2.

2.2.1 Layered based classification of threats

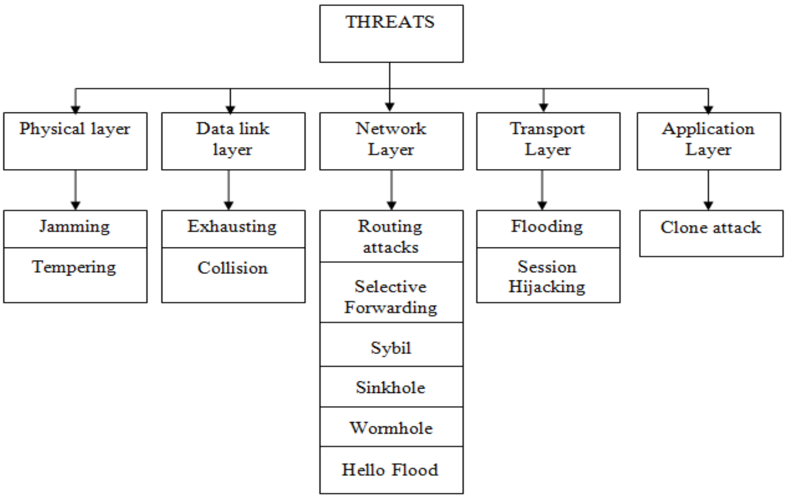


Figure 2.1: Layer Based Classification of Threat

1. Jamming: Jamming is a type of attack which interferes with the radio frequencies that a network's nodes are using. A jamming source may either be powerful enough to disrupt the entire network or less powerful and only able to disrupt a smaller portion of the network.
2. Tampering: Given physical access to a node, an attacker can extract sensitive information such as cryptographic keys or other data on the node. The node may also be altered or replaced to create a compromised node which the attacker controls.
3. Collisions: A collision occurs when two nodes attempt to transmit on the same frequency simultaneously. When packets collide, a change will likely occur in the data portion, causing a checksum mismatch at the receiving end. The packet will then be discarded as invalid.
4. Wormhole attack: One node in the network sends a message to another node in the network. Then the receiving nodeattempts to send the message to its neighbours. The neighbouringnodes think the message was sent from the sender node (which isusually out of range), so they attempt to send the message to theoriginating node, but it never arrives since it is too far away.Wormhole attacks are difficult to counter because routing information supplied by a node is difficult to verify.
5. The Sybil attack: In this attack, a single node i.e. a malicious node will appear to be a set of nodes and will send incorrect information to node inthe network. The incorrect information can be a variety of things,including position of nodes, signal strengths, making up nodesthat do not exist.Authentication and encryption techniques can prevent an outsiderto launch a Sybil attack on the sensor network. However, aninsider cannot be prevented from participating in the network.
6. Selective Forwarding attack: It is a situation when certain nodes do not forward many of the messages they receive. The sensor networks depend on repeatedforwarding by broadcast for messages to propagate throughoutthe network.
7. Sinkhole attacks: In a sinkhole attack, the adversary aim is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the Centre.
8. Passive Information Gathering:An intruder with an appropriately powerful receiver and well-designed antenna can easily pick off the data stream.Interception of the messages containing the physical locations ofsensor nodes allows an attacker to locate the nodes and destroythem.
9. Node Capturing: A particular sensor might be captured, and information stored onit might be obtained by an adversary.
10. Hello flood attacks: The Hello flood attacks can be caused by a node whichbroadcasts a Hello packet with very high power, so that a largenumber of nodes even far away in the network choose it as theparent. All messages now need to be routed multi-hop tothis parent, which increases delay.
11. Flooding: An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit.
12. False or Malicious Node: Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by thecompromised nodes within the network.

2.2.2 Classification on the basis of attack characteristics

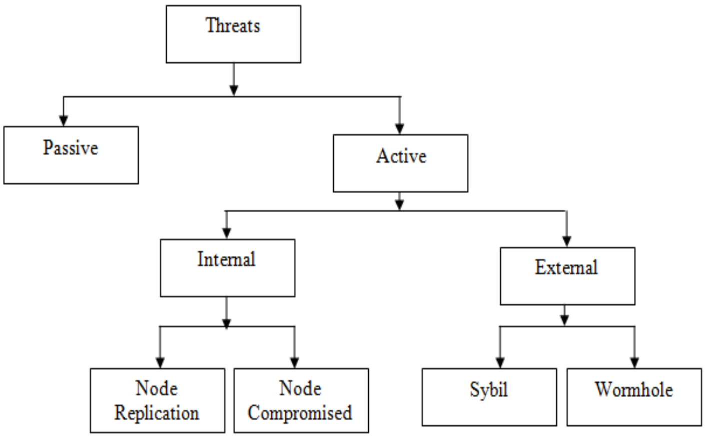


Figure 2.2: Classification based on attack characteristic

1. Passive attacks: passive attacks include eavesdropping on or monitoring packets exchanged within a WSN.
2. Active attacks: active attacks involve some modifications of the data steam or the creation of a false stream.
3. Internal attacks: insider attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways. Node replication and compromised node are the example of internal attacks.

4. External attacks: external attacks are defined as attacks from nodes which do not belong to a WSN. Sybil and wormhole attack are example of external attacks.

2.3 Defensive mechanisms in WSN

Currently, research on providing security solutions for WSNs has focused mainly in three categories:

1. Key management:A lot of work has been done in establishing cryptographic keys between nodes to enable encryption and authentication.
2. Authentication and Secure Routing:Several protocols have been proposed to protect information from being revealed to an unauthorized party and guarantee its integral delivery to the base station.
3. Secure services:Certain progress has been made in providing specialized secure services, like secure localization, secure aggregation and secure time synchronization.

2.4 WSN Security limitation

The deployment methods of WSN make them more vulnerable to various attacks. WSN are used in applications where the sensors have physical interactions with the environment and are accessible by anyone makes them more vulnerable to security threats. Due to resource constraints the IDS for traditional network can't be used directly in WSN. Several schemes are there for WSN but most of them focus on specific attacks. By using IDS we can provide second line of defence to WSN.

A wireless sensor network has many resource constraints as compared to the traditional computer networks. Due to these resource constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints first

One typical sensor network consists of nodes, small battery powered devices, which communicate with more powerful base station, which in turn connected to the outside network. The sensor networks have limited processing power, storage and bandwidth and energy. By design these sensors nodes are inexpensive, low power devices. As a result they have limited computational and communication resources. Sensor node typically consists of 8-bit 4-MHz processors with slow 10-Kbps communication and 8-Kbyte read-only memory and a 512-byte RAM. However these protocols and algorithms are too heavy weight for use in sensor network. They are having very high communication overheads and they are not designed to run on computationally constrained devices. They will also increase power consumption. So there is a need for new more energy efficient cryptographic algorithms and protocols.

III. Intrusion Detection System For Wireless Sensor Networks

3.1 Need of IDS for WSN

The defensive mechanisms are based on particular assumptions about the nature of attacks. If the attacker is“weak”, the protocol will achieve its security goal. This means that an intruder is preventedfrom breaking into a sensor network and hinders its proper operation. If theattacker is “strong” (i.e., behaves more maliciously), there is a no negligible probability that the adversary will break in. Because of their resource constraints, sensor nodes usually cannot deal with very strong adversaries. So what is needed is a second line of defence: An Intrusion Detection System (IDS) that can detecta third party's attempts of exploiting possible insecurities and warnfor malicious attacks, even if these attacks have not been experienced before.[4]

3.2 Required Features of IDS for WSN

Each sensor node has limited communication and computational resources and a short radio range. Furthermore, each node is a weak unit that can be easily compromised by an adversary, who can then load malicious software to launch an insider attack. In this context, a distributed architecture, based on node cooperationis a desirable solution. In particular, we require that an IDS system for sensor networks must satisfy the following features:[5]

1. *Localize auditing*: IDS for sensor networks must work with localized and partial audit data. In sensor networks there are no centralized points (apart from the base station) that can collect global audit data, so this approach fits the sensor network paradigm.
2. *Minimize resources*: IDS for sensor networks should utilize a small amount of resources. The wireless network does not have stable connections, and physical resources of network and devices, such as bandwidth and power, are limited. Disconnection can happen at any time.
3. *Trust no node*: IDS cannot assume any single node is secure. Unlike wired networks, sensor nodes can be very easily compromised. Therefore, in cooperative algorithms, the IDS must assume that nonode can be fully trusted.
4. *Be truly distributed*: That means data collection and analysis is performed on a number of locations. The distributed approach also applies to execution of the detection algorithm and alert correlation.

5. *Be secure*: An IDS should be able to withstand a hostile attack against itself. Compromising a monitoring node and controlling the behaviour of the embedded IDS agent should not enable an adversary to revoke a legitimate node from the network, or keep another intruder node undetected.

3.3 Different IDS for Wireless Sensor Networks

Wireless network IDS architectures into four categories. This classification can be adjusted to the needs of WSN IDS.

Classification for different IDS is presented in Figure 3.1.According to this IDS for WSN are mainly classified in following four categories:

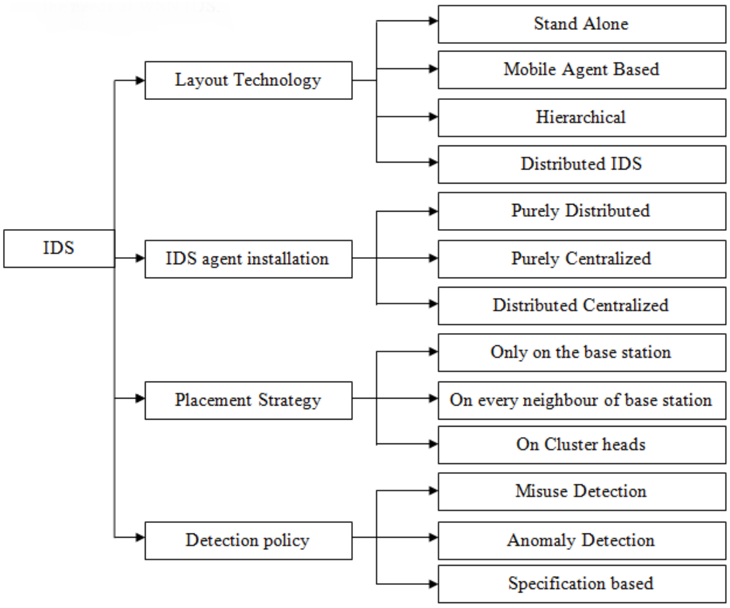


Figure 3.1: Classification of IDS for WSN

3.3.1 Layout Technology

1. Stand-alone

In this category each node operates as independent IDS and is responsible for detecting attacks only for itself.

Such an IDS does not share any information or cooperate with other systems. This architecture implies that all the nodes of the network are capable of running IDS.

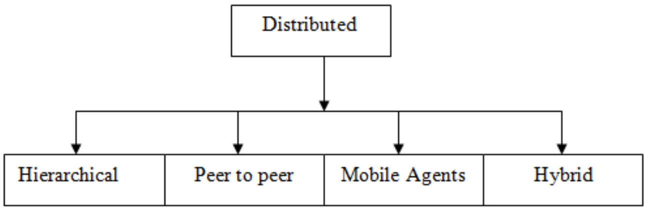


Figure-3.2: Classification of Distributed IDS

2. Distributed

Here, all nodes still are running their own IDS, but the IDS cooperate in order to create a global intrusion detection mechanism.

3. Hierarchical

In this case the network is divided into clusters with cluster-head nodes. These nodes are responsible for routing within the cluster and accept all the accusation messages from the other cluster members indicating something malicious. Additionally, the cluster-head nodes may also detect attacks against the other cluster-head nodes of the network, as they constitute the backbone of the routing infrastructure.

4. Mobile agent based

Mobile Agent Based IDSuse pieces of mobile code charged with a specific mission and sent to other nodes. Depending on the system, the mission can be to analyse the local audit data of other nodes and bringing back the results to the originator, or to run specific attack detection on a node in order to distribute the detection tasks amongst thenetwork. Mobile agents are intelligent program threads that function continuously and are able to learn, communicate and migrate themselves from host to host to gather information and perhaps perform specific tasks on behalf of a user mobile agents are dispatched to hosts where they activate the sensor there, process collected data, and send it to the main station, which signals the agents to either stop collecting data or continue, with possible changes to the collection frequency and context.

3.3.2 Installation of IDS agent

An IDS can also be classified on the basis of IDS agent installation as follows: [6]

1. Purely Distributed

In purely distributed IDS approach, IDS agent is installed in every node. It checks abnormal behaviour of neighbouring nodes locally. It analyses the data that it receives from its radio range. There are further two ways for declaring a node as compromised or not. In individualized decision making, node that detects the anomalous behaviour of another node sends that information to the sink or BS. In cooperative decision making, node that detects the anomalous behaviour of any node communicates with other nodes and finally that node is declared compromised after voting.

2. Purely Centralized

In WSNs, sensor nodes sense the environment and transmit processed information to the sink or base station. In purely centralized IDS approach, IDS agent is installed in the sink or BS. It requires an additional special routing protocol that gathers or collects information from nodes to analyse the behaviour of sensor nodes collectively.

3. Distributed Centralized

Cluster-head approach lowers the power consumption and efficiently reduces control overhead. The concept of monitor node is derived from this philosophy. In distributed centralizedapproach, IDS agent is installed in monitor nodes only. This nodeperforms two types of functions simultaneously. First, it performs activities likenormal nodes and secondly, it checks for intrusion detection. The logic behind thatapproach is to minimize the detection overhead faced by purely distributed approach.

3.3.3Placement Strategies

Different strategies are used for placing the IDS in WSN which are discussed as follows:

1. Promiscuous monitoring:

A simple strategy would be to place IDS modules in every sensor node and to have each node operate in a promiscuous mode. In this way, any malicious packet can be easily detected. However, because of the high overhead associated with this strategy, each participating node's ability to forward network traffic is severely reduced. Furthermore this IDS module placement strategy may lead to network traffic collisions and power consumption. A node monitors only the packets that pass through it. According to this placement strategy the IDS modules are also placed on every sensor node, but only the packets that pass through each sensor node are used for the analysis.

2. IDS modules on the base station

Another possible strategy would be to place the IDS modules on the base station. The base station can analyse allthe traffic in the sensor network regardless of topology or routing changes and each packet is not processed multiple times. Nevertheless, although a packet is not processed many times, this placement strategy might overwhelm the base station leading to a large number of packets not being analysed.

3. IDS modules on every neighbour of the base station

In order to reduce the computational load on the base station, IDS modules can be placed on every neighbour of the base station. However, this architecture cannot combat resource exhaustion attacks since flooding packets will only be dropped when they reach their destination.

4. IDS modules in "cluster heads"

An efficient solution for the placement of IDS modules would position the IDS monitors in such a way that all the packets would be inspected only once, in order to address the resource constraints of the sensor networks. Thus, the IDS modules could be placed in selected sensor nodes that would be able to cover all the paths from every source node to the base station. In order to achieve this, the sensor network may be divided into clusters with each cluster having a cluster head. This placement strategy implies that every member node of a cluster should forward its data packets to the cluster head which correspondingly forwards them to the base station

3.3.4 Detection policy

There are three main techniques that an intrusion detection system can use to classify actions.

1. *Misuse Detection*:

In misuse detection or signature-based detection systems, the observed behaviour is compared with known attack patterns (signatures). Action patterns that may pose a security threat must be defined and stored to the system. Then, the misuse detection system tries to recognize any "bad" behaviour according to these patterns.

2. *Anomaly Detection*:

Anomaly detection systems focus on normal behaviours, rather than attack behaviours. First these systems describe what constitutes a "normal" behaviour (usually established by automated training) and then flag as intrusion attempts any activities that differ from this behaviour by a statistically significant amount.

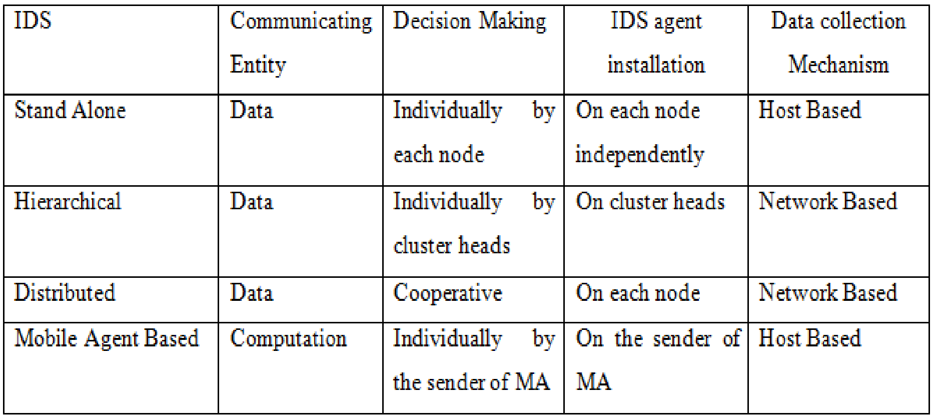
3. *Specification Based*:

Specification-based detection systems are also based on deviations from normal behaviour in order to detect attacks, but they are based on manually defined specifications that describe what a correct operation is and monitor any behaviour with respect to these constraints.

IDS agent generally include the following six components

1. One or several data collection modules obtain intrusion detection data from different sources
2. Local detection engine (also called a watchdog) analyses locally obtained trace data
3. Cooperative detection engine is used to propagate intrusion detection state information among neighbouring nodes in case local detection evidence is weak or inconclusive
4. Local response module
5. Global response module triggers different reactions, which depend on a type of the intrusion, a type of network protocol and application, and a confidence in the evidence
6. Secure communication module provides monitoring nodes with secure communication channel.

3.4 Comparative analysis of Different IDS



IDS	Communicating Entity	Decision Making	IDS agent installation	Data collection Mechanism
Stand Alone	Data	Individually by each node	On each node independently	Host Based
Hierarchical	Data	Individually by cluster heads	On cluster heads	Network Based
Distributed	Data	Cooperative	On each node	Network Based
Mobile Agent Based	Computation	Individually by the sender of MA	On the sender of MA	Host Based

Table-3.4: Comparison of different IDS

IV. DISTRIBUTED IDS FOR WSN

In Distributed IDS (DIDS) conventional intrusion detectionsystem are embedded inside intelligent agents and are deployed over a large network. In a distributed environmentIDS agents communicate with each other, or with a central server. Distributed monitoring allows early detection ofplanned and coordinated attacks and thereby allowing the network administrators to take preventive measures. DIDSalso helps to control the spreading of worms, improves network monitoring and incident analysis, attack tracing andso on. It also helps to detect new threats from unauthorized users, back-door attackers and hackers to the networkacross multiple locations, which are geographically separated. In a DIDS it is important to ensure that the individualIDS are light-weight and accurate.Distributed IDSmeet the decentralized nature of ad-hocwireless sensor networks, where each node is responsible forcollecting local audit data, and this knowledge is sharedglobally in order to carry out a global intrusion detectionsystem.

4.1 Architecture of Distributed IDS

The proposed IDS is based on a distributed intelligent agent-based system. The agents that are hosted by the nodes are capable of sharing their partial views, agree on the identity of the source and expose it. By distributing the agents throughout the network and have them collaborate, make the system scalable and adaptive. When a malicious node is found, an alarm message is broadcasted to the network. Each node then makes a final decision based on the detection reports from other nodes. To avoid drastic flooding over the network caused by broadcasting local detection results, the alarm messages are restricted to a region formed only by the alerted nodes.

The IDS architecture is based on the conceptual modules shown in Figure 4.1[7]. Our architecture consists of seven main components: Local Packet Monitoring, NbrPerimeter, Key Management, local Detection, Alert Region, Voting and Local Response. Each module is responsible for a specific function, which is described in the sections below.

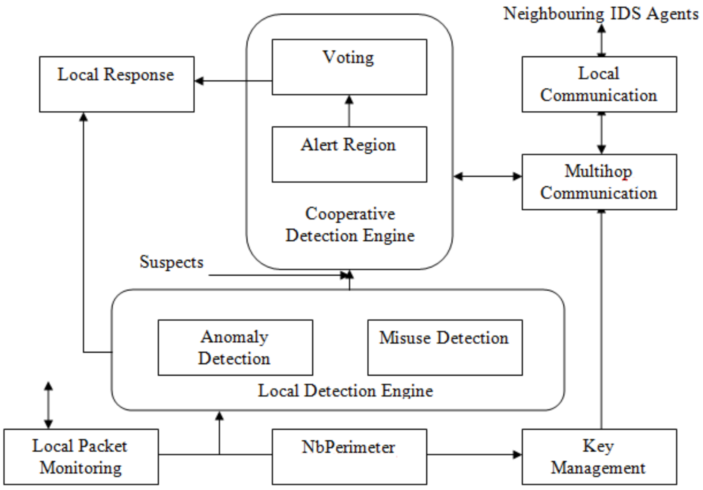


Figure 4.1: Architecture of Distributed IDS

4.1.1 Local Packet Monitoring Module

This module gathers audit data to be provided to the local detection module. Audit data in a sensor networks IDS system can be the communication activities within its radio range. This data can be collected by listening promiscuously to neighboring nodes transmissions.

4.1.2 NbPerimeter Module

This module is responsible for maintaining consistent in formation about 1-hop and 2-hop neighbors of the nodes. Information about 2-hop neighbors is needed because, the detection process involves the communication of the nodes which are neighbors of the (yet unknown) attacker, but they might be 2-hops away from each other. During an initialization phase that takes place immediately after the deployment of the network, the NbPerimeter module broadcasts the node ID and the IDs of the node's immediate neighbors within a packet that has a TTL field equal to 1, meaning that each packet will be forwarded just once by the sender's 1-hop neighbors. The discovered neighborhood information is stored in a table, which we call the 2-hops neighborhood table.

4.1.3 Key Management Module

After the deployment of the sensor network, the KeyManagementmodule of the node generates a one-way key chainof length n, using a pre-assigned unique secret key Kn. A one-way key chain (K0,K1, . . . ,Kn−1,Kn) is an orderedlist of cryptographic keys generated by successively applying a one-way hash function F to the key seed Kn, suchas Kj = F(Kj+1), for j = n to 1 Therefore, any keyKj is a commitment to all subsequent keys Ki, i > j. In this implementation, SHA-1 hashing is used for the production of the key chain. As the last step in the initializationphase,the KeyManagement module in each node announcesthe resulted K0 to all of its 1-hop and 2-hop neighbors.The KeyManagement module also stores the corresponding information for the neighboring nodes (up to 2-hops), i.e.the node IDs and their keys. This information needs to remain consistent and up-to-date during the lifetime of the network. So, the Key Management module updates the corresponding key every time a node publishes a new one from its key chain.

4.1.4 Local Detection Engine

This module collects the audit data and analyses it according to some given rules. A set of rules is provided for each attack, and whenever one or more rules are satisfied, a local alert is produced by the module. Whether a rule is satisfied or not does not just depend on information from the intercepted packets, but also on information from the 2-hop neighborhood table or information from past observed behavior.As depicted in Figure 4.1, the Local Detection Engine incorporates both classes of intrusion detection techniques, i.e., misuse detection and anomaly detection.

4.1.5 Alert Region Module

This module is activated only in the case where the Local Detection Engine module was inconclusive on the identity of the attacker and a suspects list was produced. In this case we call the node an alerted node. The set of alerted nodes define an alert region. Since not every node that belongs to the alert region has to be within communication range of each other, we need to define a communication abstraction intended to provide "connectivity" between them, or else a "neighborhood relationship".

4.1.6 Voting Module

The Voting module is responsible for executing the protocol of the voting phase, which follows after the construction of the alert region. The goal of the voting phase is to have the nodes collaborate and exchange their suspect lists, so that they can agree on the identity of the attacker.What is important here is to have honest nodes receive the votes of the rest of the honest nodes in the alert region and each vote is indeed the one transmitted by the corresponding node. To achieve this, we must ensure of two things. First, that the votes of the honest nodes do not get lost, i.e. all honest nodes receive all votes from the rest of the honest nodes. This is possible because of the alert region that we constructed in the previous phase. Each node expects to receive the votes from the rest of the nodes in the alert region. If a vote gets lost, a node can request it and receive it (given that it has at least one honest alerted neighbor). The second thing to ensure is that the votes of honest nodes do not get spoofed by intermediate faulty nodes. For this reason, each node signs the votes using the next key from its key chain.

4.1.7 Local Response Module

Once the network is aware that an intrusion has takenplace and have detected the compromised area, appropriateactions are taken by the LocalResponse module. The firstaction is to cut off the intruder as much as possible and isolate the compromised nodes. After that, proper operationof the network must be restored. This may include changesin the routing paths, updates of the cryptographic material(keys, etc.) or restoring part of the system using redundant information distributed in other parts of the network. Depending on the confidence and the type of the attack, response can be in two types:

- Direct response:

Excluding the suspect node from anypaths and forcing regeneration of new cryptographickeys with the rest of the neighbors.

- Indirect response:

Notifying the base station about theintruder or reducing the quality estimation for the linkto that node, so that it will gradually loose its path reliability.

4.2 Features of Distributed IDS

It try to generalize the problem of intrusion detection for sensor networks and build an architecture thattolerates the presence of other compromised nodes that may exist and collaborate with the attacking node in order to hinder the detection process. All nodes are loaded with the same IDS agent and they dynamically become activated around the attacking node and collaborate in order to isolate it from the network. Do not concentrate on how to detect specific attacks, although we provide a use case and the necessary modules to describe rule patterns for defending against various attacks.

Robust and scalable since each node is having its own IDS agent thus there is no single point of failure and as more nodes are added they can also work as IDS agents and collaborate with other nodes. Distributed Systems are more scalable and robust since they have different views of the network. Besides, the IDS can notice the attack fast because the monitor is near to the intruder (their distance is one hop, since the monitors were distributed in order to cover all network nodes).

Energy efficient since workload is shared on each sensor equally thus it reduces the energy consumption of each node.[8]

V. CONCLUSIONS

The objective of this work is the comparative analysis of intrusion detectioninWSNs and the associated design of IDS considering therestrictions of such networks.Intrusion detection systems, if well designed effectively can identify malicious activities and support to offer proper security. IDS for wireless sensor networks require a distributed architecture and the cooperation of nodes to make accurate decisions. Solutions must consider resource constraints in terms of computation, energy, memory, and communication.The architecture which is discussed performs decentralized detection since the IDSs are distributedon network, installed in common nodes. The collectedinformation and its treatment are performed in a distributedway. Distributed Systems are more scalable androbust since they have different views of the network.

References

[1] A. S. K. Pathan, L. Hyung-Woo, and H. Choong Seon, "Security in wireless sensor networks: issues and challenges," in *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*, 2006, pp. 6 pp.-1048.

[2] P. Inverardi, L. Mostarda, and A. Navarra, "Distributed IDSs for enhancing Security in Mobile Wireless Sensor Networks," in *Advanced Information Networking and Applications, 2006. AINA 2006. 20th International Conference on*, 2006, pp. 116-120.

[3] W. Yong, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *Communications Surveys & Tutorials, IEEE,* vol. 8, pp. 2-23, 2006.

[4] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards Intrusion Detection in Wireless Sensor Networks," Paris, April 2007.

[5] L. Besson and P. Leleu, "A Distributed Intrusion Detection System for Ad-Hoc Wireless Sensor Networks: The AWISSENET Distributed Intrusion Detection System," in *Systems, Signals and Image Processing, 2009. IWSSIP 2009. 16th International Conference on*, 2009, pp. 1-3.

[6] A. H. Farooqi and F. A. Khan, "Intrusion Detection Systems for Wireless Sensor Networks: A Survey," in *Communication and Networking*. vol. 56, D. Ślęzak, T.-h. Kim, A. C.-C. Chang, T. Vasilakos, M. Li, and K. Sakurai, Eds., ed: Springer Berlin Heidelberg, 2009, pp. 234-241.

[7] I. Krontiris, T. Giannetsos, and T. Dimitriou, "LIDeA: a distributed lightweight intrusion detection architecture for sensor networks," in *Proceedings of the 4th international conference on Security and privacy in communication netowrks*, Istanbul, Turkey, 2008, pp. 1-10.

[8] A. P. R. d. Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in *Proceedings of the 1st ACM international workshop on Quality of service ; security in wireless and mobile networks*, Montreal, Quebec, Canada, 2005, pp. 16-23.