Wireless Sensor Network based: Design Principles & measuring performance of IDS

Kamaljit Kaur
Department of IT, Guru Nanak Dev
Engg. College, Ludhiana

Bhupinder Singh
Department Mechanical,Guru Nanak
Dev Engg. College, Ludhiana

ABSTRACT

Wireless sensor networks have many potential applications for both civil and military tasks. However, sensor networks are susceptible to many types of attacks because, deployed in open and unprotected environment. For these cases, it is necessary to use some mechanism of intrusion detection. Besides preventing the intruder from causing damages to the network, the intrusion detection system (IDS) can acquire information related to the attack techniques, helping in the development of prevention systems. So it is necessary to use effective mechanisms to protect sensor networks against many types of attacks. Intrusion detection system is one of the major and efficient defensive method against attacks on wireless sensor network. Because of different characteristics of sensor networks, security solutions have to be designed with limited usage of computation and resources. In this paper different Intrusion detection systems are analyzed basis on design and performance in real time wireless sensor network environment.

I. INTRODUCTION

A wireless sensor network (WSN) is a network of cheap and simple processing devices (sensor nodes) that are equipped with environmental sensors for temperature, humidity, etc. and can communicate with each other using a wireless radio device. Sensor networks need to become autonomous and exhibit responsiveness without explicit user or administrator action. The unattended nature of WSNs and the limited resources of their nodes make them susceptible to attacks. Any defensive mechanism that could protect and guarantee their normal operation should be based on autonomous mechanisms within the network itself.

Intrusion detection is an important aspect within the broader area of computer security, in particular network security, so an attempt to apply the idea in WSNs makes a lot of sense. The architectures for (Intrusion Detection System) IDS in WSN are network-based and host-based. A network-based IDS uses raw network packets as the data source. It listens on the network and captures and examines individual packets in real time. A host-based based IDS uses the local data on host as a source to find the anomalies.

Intrusion detection systems must be able to distinguish between normal and abnormal activities in order to discover malicious attempts in time. There are three main techniques that an intrusion detection system can use to classify actions misuse detection, anomaly detection and specification based detection. In misuse detection or signature-based detection systems, the observed behavior is compared with known attack patterns (signatures). Action patterns that may pose a security threat must be defined and stored to the system. Anomaly detection systems focus on normal behaviors, rather than attack behaviors. First these systems describe what constitutes a "normal" behavior (usually established by automated training) and then flag as intrusion attempts any activities that differ from this behavior by a statistically significant amount. Finally, specification-based detection systems are also based on deviations from normal behavior in order to detect attacks, but they are based on manually defined specifications that describe what a correct operation is and monitor any behavior with respect to these constraints.

To make the final decision that a node is indeed an intruder and actions should be taken. There are two approaches for this. Either we could use a cooperative mechanism or let nodes decide independently. In an independent decision-making system, there are certain nodes that have the task to perform the decision-making functionality. They collect intrusion and anomalous activity evidences from other nodes and they make decisions about network-level intrusions. In a cooperative IDS system, if a node detects an anomaly, or if the evidence is inconclusive, then a cooperative mechanism is initiated with the neighboring nodes in order to produce a global intrusion detection action.

In this paper different IDS approaches in WSN are discussed on basis of Design and Performances parameteres.. The paper is organized as follows: Section 2 discusses the intrusion detection and decision making methodology used in different IDS's. Section 3 gives the idea about the system models of IDS's. Section 4 provides the analysis and evaluation of proposed IDS's and Section 5 concludes the paper.

II. RELATED WORK

Intrusion Detection Schemes (IDS) have often been categorized into two types: Signature-based IDS and Anomaly based IDS. From an architectural point of view, IDS schemes are further categorized into three categories: centralized, distributed and hybrid. The distributed approach is further classified into cooperative and uncooperative distributed approaches. We discuss the methodology of IDS using these schemes and architecture.

Centralized Approach

A centralized IDS is purposed by [2] to detect the DoS, which use the anomaly detection pattern for detecting potential DoS attacks. It has designed and implemented an agent-based ID on a limited set of wireless sensor nodes as a preliminary implementation. The purpose of this IDS is to discontinue communication with malicious nodes on the. For overall network status monitoring non-agent based wireless sensor node detect and display network status in the event of a DoS attack. [13] Have proposed a nice application-independent framework for identifying compromised nodes. This framework is based on alerts generated by specific intrusion detection system. The authors have adopted a centralized approach and used a simple graph theory

A different centralized uncooperative cluster approach is based on a distributed, nonparametric anomaly detection algorithm to identify anomalous measurements in nodes [9]. Sensor nodes report cluster summaries to intermediate sensor nodes, which in turn send the report in cluster form to gateway (cluster head). This scheme minimizes communication overhead. An emotional ant based approach to identify possible pre-attack activities and subsequently correspond with a centralized intrusion detection mechanism following certain knowledge base of rules depicting the probable possibilities of attack [10]. Security monitoring in the sensor network is achieved by the foraging behavior of natural ant colonies. Ants may be positioned at relevant locations in the interconnected sensor network.

A. Distributed Approach

Sheng-Tzong [1] proposed an application-independent detection model, distributed cross-layer detection model (DCD), making use of a distributed mechanism and the information of each layer in the communication protocol to detect which sensors were already compromised. Anomaly detection can detect fault detection diagnosing and malicious intruders in the WSNs. A MAC layer based intrusion detection and defense using original RTS/CTS-based MAC protocol is proposed [11]. This algorithm avoids the attack and energy wastage and doesn't require any additional hardware or cooperation among nodes. MAC protocols help to design the intrusion detection method using soft decision theory

A novel technique to optimally watch over the communications of the sensors' neighborhood on certain scenarios called spontaneous watchdogs is introduced [8]. It is a cooperative scheme which detects the abnormal behavior using knowledge and environmental database. One lightweight technique [12] use the cooperation of the agents according to the distributed nature of the events involved in the attacks, and an agent needs to send information to other agents only when this information is necessary to detect the attack. The coordination mechanism is arranged in such a way so that the distributed detection is equivalent to having all events processed in a central place using necessary modules to describe rule patterns for defending against various attacks.

A distributed and cooperative Localization Anomalies Detection (LAD) scheme [5] has proposed for the wireless sensor networks. This scheme takes the advantage of the deployment knowledge and the group membership of its neighbors, available in many sensor network applications. This information is then utilized to find out whether the estimated location is consistent with its observations. In case of an inconsistency LAD would report an anomaly. This scheme uses the deployment point.

Hybrid Approach

The perimeter surveillance as the application scenario whose aim is to provide security for high risk events that might be the target of criminal attacks. Intrusion detection WSN [7] deploy in some of the restricted areas time. The data issued by the deployed sensors can be permanently monitored in a Command and Control Center (C2C), which is able to receive in near real-time any intrusion alerts issued by the sensors. Personal Digital Assistants (PDAs) or other wireless terminals that allow direct connection to the WSN turning them into mobile sink nodes.

One another hybrid like approach is presented in which some detects intrusions cluster heads in a cluster by monitoring the messages exchanged by the sensor nodes. All messages received are analyzed using a set of rules [6]

Apart from above techniques [3] have proposed different lightweight techniques for detecting anomalies for various layers such as application, network, MAC and physical. The main advantage of proposed techniques is the low overhead that makes them energy efficient. This is due to the fact that they reuse the already available system information (e.g. RSSI values, round trip time etc.) in different layers stack.

III SYSTEM MODELS

Every IDS has its own system model according to their approaches. This model gives the insight look of working of the intrusion detection system. We are discussing the some models according to their respective approach.

A.System Models for Centralized Approach

In [2] author is aimed at establishing a basic DoS detection design that is small and simple enough to be used on any hardware. The basic architecture establish a baseline level of network traffic, and compare all future traffic to determine if a DoS attack is occurring. The IDS is setup in a similar fashion to a firewall. All outgoing and incoming traffic from the sensing applications to the network interface has to pass through the IDS allowing detection of malicious activity. Once this detection has been made the device will stop processing anything it receives from the attacker until the traffic returns to a normal level and information is sent to a mobile computer for data processing and further examination.

A cluster formation is based on the fixed-width of fixed radius w [9]. Each data vector is the Euclidean distance between the centroid of the current clusters and this data vector is computed to add or create a new cluster. Each sensor node performs the clustering operation on its own local data and sends the sufficient statistics to its immediate parent. The parent node combines the clusters from its immediate children and forms a combined set of clusters sends the sufficient statistics of the merged clusters to its immediate parent. This process continues recursively up to the gateway node. At gateway the anomaly is detected using the average inter-cluster distance of the K nearest neighbor (KNN) clusters. In which each cluster in the cluster set, a set of inter cluster distances is computed using the Euclidean distance between centroids of the number of clusters in the cluster set. Among the set of inter-cluster distances the shortest K (parameter of KNN) distances are selected and using those, the average inter-cluster distance is computed a cluster is identified as anomalous if its average inter-cluster distance is more than one standard deviation of the inter-cluster distance from the mean inter-cluster distance.

The basic idea is to identify the affected path of intrusion in the sensor network by investigating the pheromone concentration [10]. In a sensor network if the ants or emotional ants are placed, they could keep track the changes in the network path, following certain knowledge base of rules for possible attacks scenarios as suggested by the network administrator. An agent can be of the type of an object, where its function is related to the environment. At a given iteration each ant moves from the current node of sensor network to adjacent node with the maximum number of violations. A tabu list consists in nodes for every session is used to store the pheromone trace or path that is prone to attack. After visiting all nodes in the path an agent setting the degree of influence from the colony. The absolute value indicates the degree of pheromone effect. The actual validity of this rule will be examined by matching the historical data set comprised of connections marked as intruded or normal.

B. System Models for Distributed Approach

This [1] detection model includes two mechanisms that are local detection engine and cooperative detection engine. The ICDT (Individual Compromise Detection Table) stores all the information, which the local detection engine generates and uses. In addition, the ECDT (Entire Compromise Detection Table) stores all the information the cooperative detection engine uses and generates. Sensor nodes and base station collect local and global data respectively and the base station detects the compromised sensor nodes. In distributed cross-layer detection mechanism Local detection engine covers three types of detection and intrusion detection policy. 1. Check MAC layer's information i.e. schedule checking 2. Check Routing layer's information i.e. ADT checking 3. Check sensed measurements itself i.e. local measurement difference checking. This algorithm is processed in all sensor nodes. It also diagnoses which node attacker intrudes. Cooperative detection engine covers two types of detection, Fault decision policy and the last Compromise decision policy using anomaly (cross-node measurement difference) and anomaly (event response).

There is two function modules in [11]: intrusion detection and intrusion defense. Each node executes these two modules separately and automatically. Cooperation among nodes are not required, therefore it is a distributed method. Unusual changes of sensitive data elements are chosen to trigger the intrusion detection. It chooses Collision Ratio, Probability of Data Packet Successful Transmission, Data Packet's Waiting-Time, RTS Packets Arrival Ratio statistics as intrusion indicators and attacks. A threshold is defined for these four probabilities and if the combined probability is bigger than threshold then intrusion detection module announces that there is an attack found. When intrusions are found, the defense part starts to work, using some countermeasure to reduce the effects of attackers on the network.

The architecture of [8] divided into two parts: local agents and global agents. Local agents monitor the local activities and the information sent and received by the sensor. Global agents watch over the communications of their neighbors, and can also behave as watchdogs. However, not all nodes can perform this operation at the same time, only a certain subset of the nodes watches over the network communications at a time. Every node stores information about its surroundings and has an internal alert database, which is used for storing the security information generated by the node agents. Both local and global agents reside in the same node, thus the results of their observations are stored in a single alert database. As a result, collaboration between global and local agents in the same node is achieved. A local agent detects attacks against the physical or logical safety of sensor. For every packet, there are sets of nodes that are able to receive both that packet and the relayed packet by the next-hop; all these nodes activate their global agents in order to monitor those packets. They can be prepared to detect whether a certain node is dropping or modifying packets by analyzing those packets.

The proposed IDS is based on a distributed intelligent agent-based system identical in each node [12]. 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. When a malicious node is found, an alarm message by alerted nodes is broadcasted to the network. Each node then makes a final decision based on the detection reports from other nodes. This architecture contains different modules: Local Packet Monitoring Module This module gathers audit data to be provided to the local detection module. NbPerimeter Module is responsible for maintaining consistent information about 1-hop and 2-hop neighbors of the nodes. Key Management Module generates a one-way key chain of length n, using a pre-assigned unique secret key. Local Detection Engine module collects the audit data and analyzes it according to some given rules. A set of rules is provided for each attack. Alert Region Module is activated only in the case where the Local Detection Engine module was inconclusive on the identity of the attacker and a suspect's list was produced. In this case we call the node an alerted node. Voting Module is responsible for executing the protocol of the voting phase, after the construction of the alert region, to exchange there suspect lists (votes), so that they can agree on the identity of the attacker. Local Response Module cut off the intruder as much as possible and isolates the compromised nodes after detection of intruder and compromised node.

This scheme presents a model for a type of group based deployment of sensor nodes [5]. A deployment point of a sensor is the point location where the sensor is to be deployed and a resident point of a sensor as the point location where the sensor finally resides. In a group-based deployment, sensor nodes to be deployed are divided into n equal-size groups and deployment points are arranged in a grid. During deployment, the resident point of a node follows a probability distribution function. Three metrics are used to measure the degree of inconsistency between a node's derived location and its observation. For each metric, threshold is obtained through training. The Difference Metric represent a sensor node's estimated location derived using certain localization scheme The Add-all Metric use the total number of neighbors in the union observation as another anomaly indicator such that if groups are similar then they are closed after union otherwise far different from each other. The Probability Metric on its estimated location, the sensor can calculate how likely it can have neighbors from group. Too small probability indicates a potential anomaly. If the level of inconsistency exceeds such a threshold, it claims that the localization results are inconsistent with the observation, thus an alarm will be raised.

C. System Models for Hybrid Approach

The overall system architecture, divided into three distinct layers [7]: Application layer, which directly supports the security forces application. It contains distributed shared memory data storage due to its inherent replication. An event mechanism allows the definition of thresholds and actions that need to be executed. The protocol layer supports the local distribution of replication messages and also of event messages. The Destination-Sequenced Distance-Vector (DSDV) routing protocol is used for local broadcast and the Distributed Transport for wireless Sensor Networks (DTSN) transport protocol ensures reliable data transport. The target system layer provides services such as memory Management and also supports security mechanisms used by the application providing implementations of cipher means. The event mechanism in monitors the chosen Variables, which is defined as a logic equation with several possible predefined Boolean resulting operations. In case the logic equation results in logic true, the Event & Replication Logic fires an event depending on the configured policy.

This model presents decentralized and energy efficient intrusion detection system using In Rule based detection and "cluster-first" protocol [6]. First cluster are formed and then the cluster-heads are elected. The protocol evolves in four basic steps: The first step consists of the exchange of the neighbor lists between the neighbors and the computation of the local maximum clique (cluster) by each of the nodes. In the second step, each node exchanges its local maximum clique with its neighbors, and adjusts its maximum clique In the third step, each node exchanges the updated clique with its neighbors, and derives its final clique. In step four, the neighbors exchange their final cliques. If a clique inconsistency is detected, a fifth step is initiated to perform conformity checking. If a malicious neighboring node is identified, it is removed from the network, and the protocol restarts from step one and then the cliques are finalized. In Rule based detection all messages received are analyzed using set rules. If a message violates one of these rules, an alarm is raised. If the number of alarms for a specific node is above a given threshold the node is treated as an intruder. If cluster head gives the alarm the given threshold, then the cluster head is revoked and a new cluster-head is elected

IV COMPARISON AND ANALYSIS

We have summarized the existing proposed IDS schemes of WSNs according to their approaches in their respective tables.

TABLE I
SUMMARIZATION OF PROPOSED CENTRALIZED IDS

		[7]	[6]
Classification	Techni-que	Statiscal Based	Statiscal/ Rule Based
	Architecture	Hybrid	Hybrid
Specification	Installation of IDS	On Mobile Sink Nodes	On cut set of Cluster
	IDS Scope	App. Layer	Network Layer
	Attack Detects	Criminal Attack	Jamming, Radio Interference Dropping Packet Etc.
Network	Sensor node	Static/Mobile	Static
	Topo-logy	Tree	Any

In table1 [2][13][9][10] proposed centralized IDS's, which can detect some particular attack or based on the rules, which are set in the node or cluster head. However centralized approach reduce the overhead of every node to watch and detect the anomalies but at the cost. First a centralized node should have an extra computation power and energy. Secondly it is the center of attraction of any intruder. Failure of node can make the network insecure. It can be good choice where network is static, small and need the low cost deployment.

In table2 [1][11][8][5] proposed IDS based on the distributed approach. Most of them use the statiscal approach to detect the intrusion or anomaly. In distributed approach every node contain the IDS using a node detect the attacks. This approach keeps the node alive however in some schemes only particular nodes are active at a time. Node has to calculate, match the pattern and check the threshold and if any abnormal activity found then node raise the alarm and take the action. This approach is also useful when network is dynamic and can be scaleable. Moreover if adversary attacks in different parts of the network even then attack can be detected and defended. Only problem is that every node has to do the extra task and computation.

TABLE 2
. SUMMARIZATION OF PROPOSED DISTRIBUTED IDS

		[1]	[11]	[8]	[5]
Classification	Technique	Signature Based	Statiscal Based	Signature/ Statiscal Based	Statiscal Based
	Architecture	Distributed Cooperatve	Distributed	Distributed	Distributd Cooperatve
Specification	Installation of IDS	On every Sensor Node	On Every Sensor Node	On Every Sensor Node	On every Sensor Node
	IDS Scope	Multi layer	MAC layer	Network Layer	App. Layer
	Attack Detects	Fault detection/ anomalies	Collision, Unfairness, Exhaustion	Spurious Injection etc.	Localization anomalies
Network	Sensor node	Static	Static	Static	Static
	Topology	Any	Any	Tree Based	Any

TABLE 3
. SUMMARIZATION OF PROPOSED DISTRIBUTED IDS

		[2]	[13]	[9]	[10]
Classification	Technique	Rule Based	Statiscal Based	Statiscal Based	Rule Based
	Architecture	Centralized	Centralized	Centralized	Centralized
Specification	Installation of IDS	Special IDS Node	On Every Cluster Head	On Every Cluster Head	At relevant Locations
	IDS Scope	Network Layer	Multi layer	Network Layer	Network Layer
	Attack Detects	Flooding	Jamming, Exhaustion Misdrection Flooding	Correlated anomalies	Correlated anomalies
Network	Sensor node	Static	Static	Static	Static
	Topology	Any	Any	Tree Based	Any

In table3 [7][6] proposed hybrid architecture, which uses the mixture of above said approach In which detection part done by the nodes and action is taken by sink node or base station. However it seems that this approach uses the advantages of both above said approaches but this is not true. Because base station can be fixed or mobile and message or report about the sent to the base station requires extra secure communication, integrity and authentication scheme so that base station can be able to differentiate the false reports.

V CONCLUSION

In this paper we have discussed about proposed IDS in WSN and discussed different approaches used in the IDSs. Then some system models have been discussed which are based on the approaches and finally comparison and analysis has been done of all approaches. However all approaches has their own strengths and weaknesses but distributed approach is more deserving if we consider the resource constraints of WSN and want to secure the network using those constraints.

REFERENCES

[1.] Sheng-Tzong Cheng; Szu-YunLi; Chia-Mei Chen, “Distributed Detection in Wireless Sensor Networks”, Computer and Information Science, 2008. ICIS 08. Seventh IEEE/ACIS International Conference, pp.401 – 406, 2008.

[2.] Martynov, D. Roman, J. Vaidya, S, “Design and implementation of an intrusion detection system for wireless sensor networks”, Electro/Information Technology, 2007 IEEE International Conference on , Chicago, pp507 – 512, 2007.

[3.] V. Bhuse and A. Gupta, “Anomaly intrusion detection in wireless sensor networks,” Journal of High Speed Networks, vol. 15, no. 1, pp. 33–51, 2006.

[4.] Shaikh, R.A.; Jameel, H.; d'Auriol, B.J.; Sungyoung Lee; Young-Jae Song; Heejo Lee,“Trusting Anomaly and Intrusion Claims for Cooperative Distributed Intrusion Detection Schemes of Wireless Sensor Networks”, Young Computer Scientists, 2008. The 9th International Conference, pp2038-2043. 2008.

[5.] W. Du, L. Fang, and N. Peng., “ LAD: Localization Anomaly Detection For Wireless Sensor Network.”, Journal of Parallel and Distributed Computing, 66:874–886, 2006.

[6.] Chatzigiannakis, I.; Strikos, “A Decentralized Intrusion Detection System For Increasing Security Of Wireless Sensor Networks” A. Emerging Technologies and Factory Automation, 2007. ETFA. IEEE Conference , pp1408 – 1411, 2007

[7.] Langendorfer, P.; Grilo, A.; Piotrowski, K.; Casaca , “A Wireless Sensor Network Reliable Architecture for Intrusion Detection” A Next Generation Internet Networks, pp189 – 194, 2008

[8.] Roman, R. Jianying Zhou Lopez, J., “Applying Intrusion Detection Systems To Wireless Sensor Networks” 3rd IEEE Consumer Communications and Networking Conference, Vol. 1, pp640- 644, 2006.

[9.] Sutharshan Rajasegarar; Christopher Leckie; Marimuthu Palaniswami; James C. Bezdek, “ Distributed Anomaly Detection in Wireless Sensor Networks”, 10th IEEE Singapore International Conference on Communication systems, pp1 – 5, 2006.

[10.] S Banerjee, C Grosan, A Abraham, “ IDEAS: Intrusion Detection Based On Emotional Ants For Sensors “, Proceedings. 5th International Conference on Intelligent Systems Design and Applications, pp. 344-349, 2005

[11.] Qingchun Ren; Qilian Liang, “Secure Media Access Control (MAC) In Wireless Sensor Networks: Intrusion Detections And Countermeasures”,15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Vol. 4, pp 3025 – 3029, 2004.

[12.] Ioannis Krontiris, Thanassis Giannetsos, Tassos Dimitriou, “LIDeA: A Distributed Lightweight Intrusion Detection Architecture For Sensor Networks”, Proceedings of the 4th international conference on Security and privacy in communication networks, 2008.

[13.] Q. Zhang, T. Yu, and P. Ning., “A Framework For Identifying Compromised Nodes In Wireless Sensor Networks.”, ACM Trans. Inf. Syst. Secur., pp1–37, 2008.