IJRSET OCTOBER 2018 Volume 5, Issue 10 Pages: 13-19

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

SPY IDENTIFICATION AND INTRUSION DETECTION SYSTEM FOR WIRELESS SENSOR NETWORKS

[1] Rajeswari M, [2] G. Dalin
[1] Research Scholar, [2] Research Supervisor,
[1, 2] Hindusthan College of Arts and Science, Coimbatore, Tamilnadu, India.

ABSTRACT: Intrusion detection is the one of the major problem in network security, as the use of computer system and network increases, securing data is one of the important in order to achieve secure data transmission without hacking. Intrusions are the activities that violate the security policy of system. The process used to identify intrusions. Today network securities are used in various applications like protect vital information while still allowing access to those who need Trade secrets, Medical records etc. In this paper proposed to a novel hybrid intrusion detection framework methodology and its four various level of phases. we proposed a novel method; different techniques are proposed to effectively detect the malicious attack in network in four phases.. The proposed method provides good result than comparing with existing method.

Keywords: [Wireless sensor network, load balancing, network initialization, spy detection, IDS Spy detection.]

1. INTRODUCTION

Wireless Sensor Networks have been applied to a range of applications, monitoring of space which includes environmental and habitat monitoring, indoor climate control, surveillance. Monitoring things example can be outlined as structural monitoring, condition- based equipment maintenance. In addition, monitoring the interactions of things with each other and the surrounding space e.g., emergency response, disaster management, healthcare, energy sector. The majority of these applications may be split into two classifications: data collection and event detection. In various applications of WSNs, the node deployment always draws attention to cover the area of interest. Node deployment strategy is a fundamental issue of a WSN provisioning that is done based on the implementation scenario. The types, number, and locations of devices impact on many intrinsic properties of a WSN, such as coverage, connectivity, cost and lifetime. Recently, the WSN‟s technology has widely been used in our daily life. A typical WSN is shown in Figure 1. In Figure 1 an event is detected in the sensor field and the information is routed to the sinker or base station then to the user with several communication media. Deployment can normally be categorized as either a dense deployment or a sparse deployment. A dense deployment has a relatively high number of sensor nodes in a given field of interest while a sparse deployment would have fewer nodes in the same field.

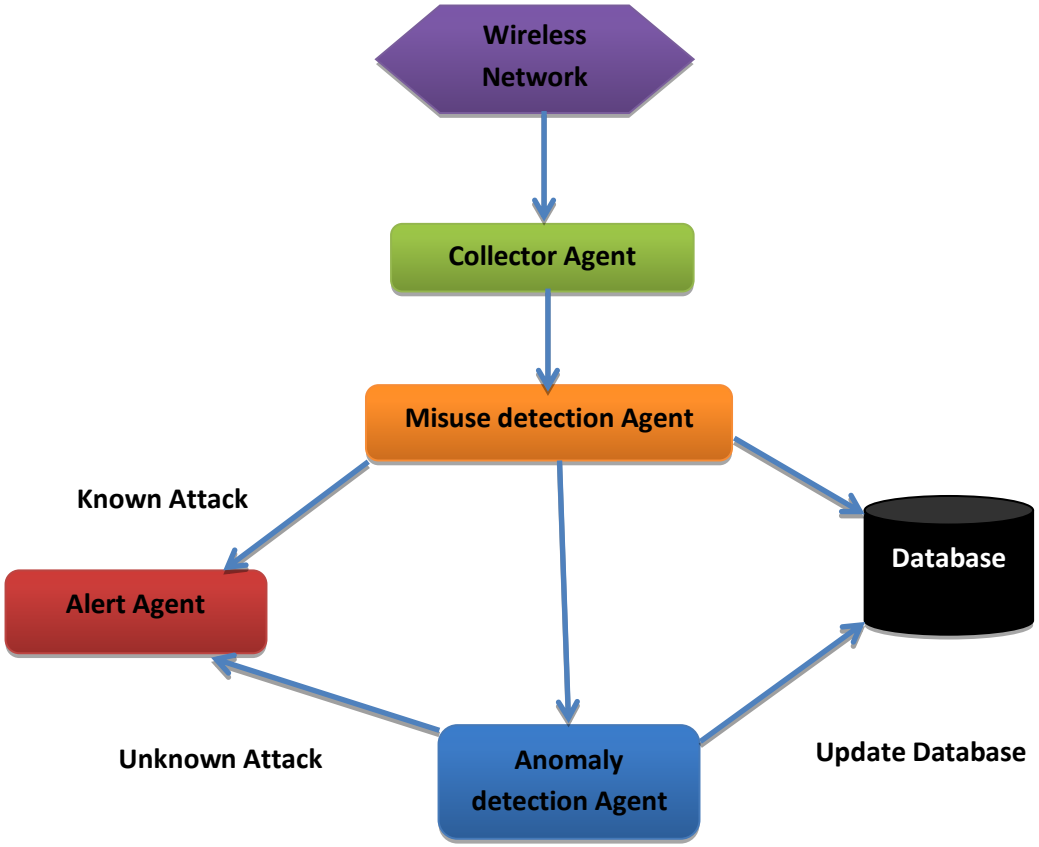

Figure 1: System Architecture for WSN

2. INTRUSION DETECTION

WSNs comprise of nodes having restricted resources and therefore classical security measures pertinent in customary networks can't be applied here. So the need of great importance is utilizing systems that exist in the limit of the sensor nodes resource potential too skilled enough to deal with attacks. Intrusion detection is one such guard utilized in sensor networks being able to recognize obscure attacks and discovering intends to defeat them. Researchers have discovered intrusion detection system (IDS) to be a lot of viable in sensor networks. Therefore intrusion detection holds a conspicuous research area for researchers. So knowledge of this promising research field will surely profit the researchers. Remembering this we review the significant subjects of intrusion detection in WSNs. The administrative work presents points, for example, the compositional models utilized in the different methodologies for intrusion detection, different intrusion detection techniques and spy distinguishing proof strategies pertinent for the different layers in sensor networks.

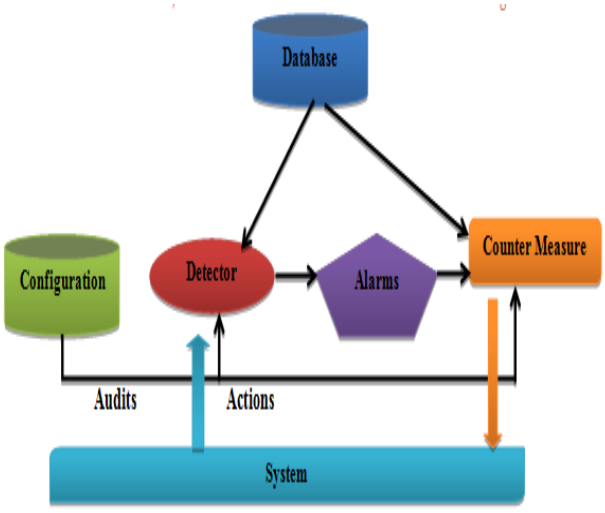

Figure 2: Block Diagram for Intrusion Detection System

Spy Sense

Spy-Sense exploits will reside in a ceaseless memory region in the host sensor stage. They can work in secretive mode as they are programmed to change and restore the flow

of the system's control in quite a manner with the goal that they don't release the fundamental micro-controller into a precarious state. These exploits utilize the presence of an unfilled memory region reserved to be utilized as the store for dynamic memory allocation. Since business sensor stages don't uphold dynamic memory allocation, this address region between the store and the stack will remain vacant, unused and unchecked during program execution. This fills in as an umbrella of the relative multitude of exploits masquerading their reality and reliably avoiding detection.

The challenging of designing IDS for WSN

The IDS arrangements created for wired networks can't be applied directly to sensor networks, see the difference between these two sorts of networks, this is the reason it is important to present an intrusion detection system that meets the unique features of sensor networks. The plan of this sort of system for wireless sensor network must fulfill the following properties: Monitoring component Analysis Detection Alarm Figure 2. Testing of planning IDS for WSN.

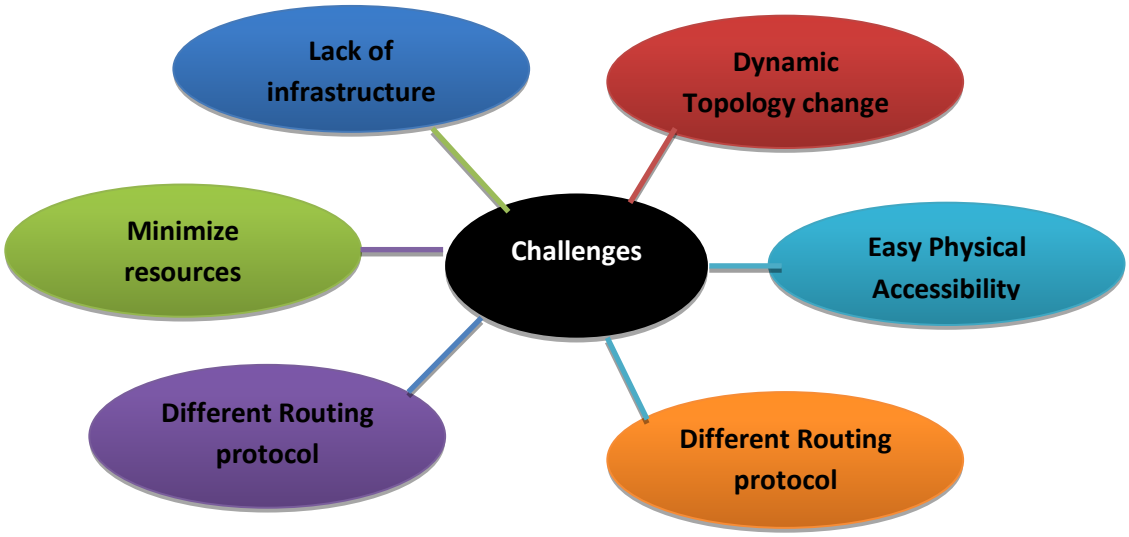

Figure 3: Challenges of IDS

3. EXISTING SYSTEM

1. Rule-based IDS

Rule-based IDS called additionally Signature-based IDS, explains on a database of stored earlier rules of security attacks. The majority of the techniques in these schemes follow three fundamental phases: data acquisition phase, rule application phase and intrusion detection phase. The algorithm incorporates three steps for identifying intrusions. In the initial step monitor nodes monitors the data. In the second step detection rules will be positioned arranged by seriousness, to the gathered information to hail failure. The third step is the intrusion detection phase, where the quantity of failure hailed is compared to the normal number of the occasional failures in the network.

2. Cluster-Based IDS

Cluster-Based IDS has proposed two approaches to improve the security of clusters for sensor networks utilizing IDS. The primary approach utilizes a model-based on authentication, which can resist to outside attacks. Its fundamental procedure is to add a message authentication code (MAC) for each message. At whatever point a node needs to send a message, it adds to it a timestamp and a MAC is created by a key pair or independently depending on the key part of the sender (cluster-head, part - node, or base station). With the goal that the receiver can check the sender, the security instrument is utilized LEAP. The subsequent scheme is called Energy-Saving. This approach centers on the detection of misbehavior both in Member nodes (MN) and cluster-head nodes (CH). At the point

when misbehavior is recognized, the CH communicates an admonition message encrypted with the cluster key to restrain this particular node.

3. Hybrid IDS

In the Hybrid Approach, the two techniques (Cluster-Based and Rule-Based) are consolidated to shape Hybrid detection strategy. Hybrid detection exploits the benefits of the two approaches gives straightforwardness, high wellbeing, low consumption of energy. The Hybrid Intrusion Detection System accomplishes the objectives of high detection rate and low bogus positive rate. Hybrid IDSs are commonly not recommended for resource imperative networks, for example, a WSN; anyway they are as yet a functioning research area. A hybrid intrusion detection model is presented in. In this model, sensor nodes are separated into hexagonal regions like cell networks. Every region is monitored by a cluster node, while cluster nodes are monitored by regional nodes. The base station has the responsibility to monitor every single regional node. It is progressive in nature framing a tree-like structure. Attack signatures are stored in base station and engendered toward the leaf node for attack detection. Additionally the system has predefined details of typical and irregular conduct. Anomaly detection is finished by estimating deviation from characterized details.

4. Anomaly-Based Intrusion Detection Systems

Anomaly-based IDS monitors' network exercises and groups them as one or the other ordinary or malicious utilizing heuristic approach. The vast majority of anomaly-based IDSs recognize intrusions utilizing threshold values; that is, any action below a threshold is typical, while any condition over a threshold is named an intrusion. The fundamental preferred position of anomaly-based IDS is its capacity to identify new and obscure attacks; anyway at times it neglects to recognize even notable security attacks. Some anomaly-based IDSs have been proposed up until this point. An unsupervised neural network based IDS [34] is fit for learning and distinguishing obscure attacks. This smart system learns the time-related changes utilizing Markov model. At the point when any intrusion happens, a versatile specialist moves to the malicious region of the WSN to explore. The proposed system can identify time-related changes and occasions.

4. PROPOSED SYSTEM

SPY AGENT

The SPY Agent (SA) is the key element in our proposed architecture. The SA is a moving agent which moves around the network and monitors the Cluster Head's (CHs) status, CH status implies it checks whether the CH is in dynamic state or the CH node has sufficient measure of energy to proceed with the aggregation process. In the event that any of the above conditions are bombed implies immediately the SPY Agent effectively will takes an interest in Weak CH identification and recovery process. The SPY Agent contains the following fields.

CH ID	Life Time (LT)	Residual Energy(RE)

Table 1: SPY Agent Fields

In the above Table.1, CH ID characterizes the Cluster head identification number. Life Time (LT) characterizes the all out life time of the nodes in the network and Residual Energy characterizes the nodes energy level value. This life time value is utilized for finding the cutting edge Cluster Head nodes from the prior existing network environment i.e, toward the end of previous aggregation process the SA will checks the LT value, in the event that one node or CH has high LT value implies that nodes will be chosen as a CH for the future.

SPY AGENT ALGORITHM

Step 1: Initially the Spy Agent (SA) moves around the network.

Step 2: SA updates its SA Field table [i.e., the CH-ID, Life Time (LT) Value and Residual Energy (RE)]

Step 3: Check, if the Residual Energy (RE) < Threshold (T)
Step 4: If yes, the CH will mark as weak CH and losses its votes
Step 5: Otherwise the SA moves to the next CH and repeat step (2) to (4).

Residual Energy:

The residual energy (RE) of each node (Ni) is calculated by using the following formula.

RE=Ei – (Etx + Erx + Ea)

Where,

RE - Residual Energy

Ei - Initial Energy of Each node

Etx - Energy used at the hour of transmission

Erx - Energy used at the hour of data reception

Ea-Energy required keeping the node dynamic

The following flow chart shows about the SPY Agent Process. The Proposed architecture and the SPY Agent algorithm are clarified through the above flow chart. The security for the data transmission is achieved through efficient encryption and decryption mechanism which is clarified in.

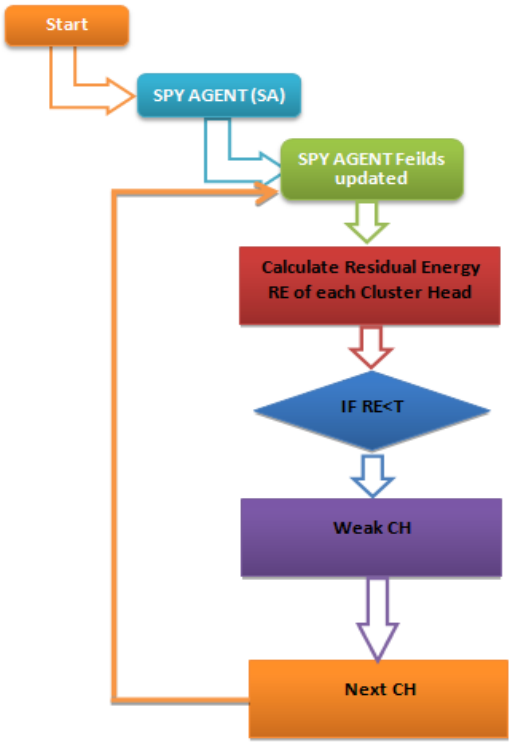

Figure 4: Flow Diagram for SPY Agent Process

Simulation Model and Parameters

The Network Simulator (NS2) is utilized to recreate the proposed architecture. In the simulation, the portable nodes move in a 500 meter × 500 meter region for 50 seconds of simulation time. All nodes have a similar transmission range of 250 meters. The reenacted traffic is Constant Bit Rate (CBR). The simulation settings and parameters are summed up in Table 2.

No. of Nodes	20,40,60,80 and100
Area Size	500 × 500
Mac	IEEE 802.11
Transmission Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Rate	50,100,150,200 and 250kb
Initial Energy	10.1J
Transmission Power	0.660
Receiving Power	0.395
Routing Protocols	AODV and DSDV

Table 2: Simulation Settings and Parameters

The proposed SPY Agent based secure data aggregation is broke down for proactive and reactive protocols. Here we have taken AODV and DSDV protocols. The presentation is assessed principally, as indicated by the following measurements.

Packet Delivery Ratio: It is the ratio between the quantity of packets received and the quantity of packets sent.

Packet Drop: It refers the normal number of packets dropped during the transmission

Residual Energy: It is the energy level remains in each node after the flow transmission.

Delay: It is the measure of time taken by the nodes to transmit the data packets.

From the above results we can break down the efficiency of our proposed methodology for the proactive routing protocol and reactive protocols for different number of nodes situation and can examine the efficiency of our proposed methodology for the proactive routing protocol and reactive protocols for different rate situation. In this paper we have proposed SPY Agent

based data aggregation in Wireless sensor network.

CONCLUSION

While planning a security mechanism, we should think about the restricted resources of WSNs. Anomaly-based IDSs are lightweight in nature; anyway they create more bogus alarms. Signature-based IDSs are appropriate for relatively huge estimated WSNs; anyway they have a few overheads such as updating and embedding new signatures. Cross layer IDSs are generally not recommended for networks having resources limitations, as more energy and calculation are required for exchanging multilayer parameters. In here the SPY agent moves around the network and checks the status of each cluster head whether the cluster head is accessible to transmit the data to the Sink or the cluster head is in feeble state based on their status. In this phase examined the proposed architecture for two different routing protocols. In future we have the arrangement to improve our SPY agent based secure data aggregation scheme by utilizing some standard encryption and decryption techniques.

REFERENCE

[1]. T. LathiesBhaskerAnd G. Arul Jagan, "Spy Agent Based Secure Data Aggregation In Wsn", Issn: 2229-6948(Online), Doi: 10.21917/Ijct.2014.0146, 2014.

[2]. Amrita Ghosal and SubirHalder," Intrusion Detection in Wireless Sensor Networks: Issues, Challenges and Approaches ", 2016.

[3]. Nabil Ali Alrajeh,1S. Khan,2and Bilal Shams, "Intrusion Detection Systems in WirelessSensor Networks: A Review", Volume 2013, Article ID 167575,7pageshttp://dx.doi.org/10.1155/2013/167575, 2013.

[4]. H.Deng,Q.A.Zeng,andD.P.Agrawal,"SVM-basedintrusiondetection system for wireless ad hoc networks," inProceedingsof the 58th IEEE Vehicular Technology Conference (VTC '03),pp.2147–2151, October 2003.

[5]. ThanassisGiannetsos, TassosDimitriou ," Spy-Sense: Spyware Tool for Executing Stealthy Exploits against Sensor Networks", 2018.

[6]. G.Gurusamy1 ,S.Shaik Majeeth2 , G.Ashok kumar3, "Spying In Wireless Sensor Network to Catch Misbehaviour Nodes", ISSN 2278 – 8875, Vol. 1, Issue 2, August 2012.

[7]. Andreas A. Strikos, "A full approach for Intrusion Detection in Wireless Sensor Networks", School of Information and Communication Technology , Stockholm, Sweden ,March 1, 2007.

[8]. R. Roman, J. Zhou, J. Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks", Proceeding of the 3rd IEEE Consumer Communications and Networking Conference, 2006.

[9]. Roosta, Tanya, Sameer Pai, Phoebus Chen, Shankar Sastry, and Stephen Wicker. "Inherent security of routing protocols in ad-hoc and sensor networks." In Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE, pp. 1273-1278. IEEE, 2007.

[10]. C.-C. Su, K.-M. Chang, Y.-H. Kuo, and M.- F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks", in 2005 IEEE Wireless Communications and Networking Conference, WCNC 2005: Broadband Wirelss for the Masses - Ready for Take-off, 2005.

[11]. Mr.Ansar I SheikhMr. PankajKewadkar, "Approach towards Intrusion Detection System for Wireless Sensor Network", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, 2013.

[12]. Misra, S., Krishna, P. V., Abraham, K. I.: Energy Efficient Learning Solution for Intrusion Detection in Wireless Sensor Networks. In: Proceedings of 2nd Int'l Conference on Communication Systems and Networks, pp. 1-6 (2010).

[13]. Mostarda, L., Navarra, A.: Distributed Intrusion Detection Systems for Enhancing Security in Mobile Wireless Sensor Networks. Int'l Journal of Distributed Sensor Networks 4(2), 83–109 (2008).

[14]. Shin, S., Kwon, T., Jo, G. –Y., Park, Y., Rhy, H.: An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks. IEEE Transactions on Industrial Informatics 6(4), 744–757 (2010).
[15]. Abduvaliyev, A.K Pathan, J. Zhou, R. Roman and W. Wong, "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks", Communications Surveys & Tutorials, IEEE Volume 15, Issue 3, 2013.