International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.113.08

Hybrid Intrusion Detection for Wireless Sensor Networks

Sadhana S. Kekan[1]
[1]*Assistant Professor, MIT COE, Pune, Maharashtra, India.*

Abstract- In recent years, the use of mobile ad hoc networks (MANETs) has been widespread in many applications, including some mission critical applications, and as such security has become one of the major concerns in MANETs. Due to some unique characteristics of MANETs, preventionmethods alone are not sufficient to make them secure; therefore, detectionshould be added as another defense before an attacker can breach the system. In general, the intrusion detection techniques for traditional wirelessnetworks are not well suited for MANETs. However, sensor networks are susceptible to many types of attacks because they are deployed in open and unprotected environment. So it is necessary to use effective mechanisms to protect sensor networks against many types of attacks on routing protocols.

Intrusion detection is one of the major and efficient defense methods against attacks in a computer network and system. Because of different characteristics of sensor networks, security solutions have to be designed with limited usage of computation and resources. In this paper, we proposed a hybrid, lightweight intrusion detection system integrated for sensor networks. Our intrusion detection scheme take advantage of cluster-based protocol to build a hierarchical network and provide an intrusion framework based both on anomaly and misuse techniques. Our scheme can prevent most of routing attacks on sensor networks.

Keywords: Intrusion detection, security, routing attacks, wireless sensor networks.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring network that is formed automatically by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. Each node is equipped with a wireless transmitter and receiver, which allow it to communicate with other nodes in its radio communication range. In order for a node to forward a packet to a node that is out of its radio range, the cooperation of other nodes in the network is needed; this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology frequently changes due to the mobility of mobile nodes as they move within, move into, or move out of the network.Multi-hop routing is a type of communication in radio networks in which network coverage area is larger than radio range of single nodes. Therefore, to reach some destination a node can use other nodes as relays[1]. Since the transceiver is the major source of power consumption in a radio node and long distance transmission requires high power, in some cases multi-hop routing can be more energy efficient than single-hop routing.

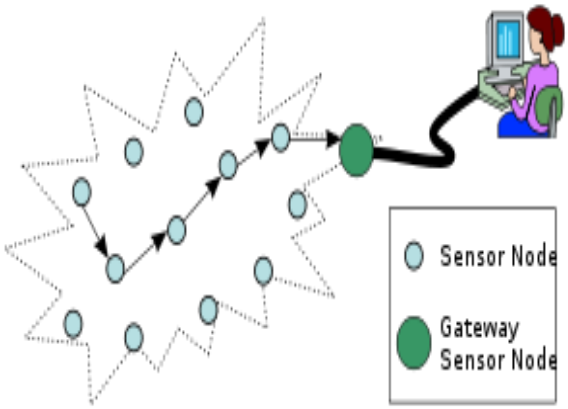

Fig 1: Typical multi-hop wireless sensor networkarchitecture

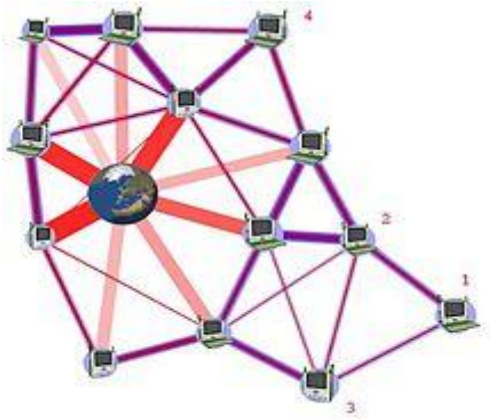

Fig 2: A wireless mesh networkarchitecture

wireless mesh network architecture allowing otherwise out-of-range nodes 1–4 to still connect to the Internet. A key characteristic is the present of multiple-hop links and using intermediate nodes to relay packets for others.

As MANETs become widely used, the security issue has become one of the primary concerns. For example, most of the routingprotocols proposed for MANETs assume that every node in the network is cooperative and not malicious [2]. Therefore, only one compromised node can cause the failure of the entire network.
There are both passive and active attacks in MANETs. For passive attacks, packets containing secret information might be eavesdropped, which violates confidentiality. Active attacks, including injecting packets to invalid destinations into the network, deleting packets, modifying the contents ofpackets, and impersonating other nodes violate availability, integrity, authentication, and non-repudiation. Proactive approaches such as cryptography and authentication here taken into consideration, and many techniques have been proposed and implemented [4]. However, these applications are not sufficient. If we have the ability to detect the attack once it comes into the network, we can stop it from doing any damage to the system or any data. Here is where the intrusion detection system comes in.
Intrusion detection can be defined as a process of monitoring activities ina system, which can be a computer or network system. The mechanism bywhich this is achieved is called an intrusion detection system (IDS). An IDS collects activity information and then analyzes it to determine whether there are any activities that violate the security rules. Once an IDS determines that an unusual activity or an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator[3]. In addition, IDS can also initiate a proper response to the malicious activity.
Although there are several intrusion detection techniques developed forwired networks today, they are not suitable for wireless networks due to the differences in their characteristics. Therefore, those techniques must be modified or new techniques must be developed to make intrusion detection work effectively in MANETs.
In this paper, we classify the architectures for IDS in MANETs, each of which is suitable for different network infrastructures. Current intrusion detection systems corresponding to those architectures are reviewed and compared.
Intrusion detection can be classified based on audit data as either host-based or network-based. A network-based IDS captures and analyzes packets from network traffic while a host-based IDS uses operating system or application logs in its analysis. Based on detection techniques, IDS can also be classified into three categories as follows,
Anomaly detection systems: The normal behaviorsof users are kept in the system. The system compares the captured data with these problems, and then treats any activity that deviates from the baseline as a possible intrusion by informing system administrators or initializing a proper response.
Misuse detection systems: The system keeps patterns (or signatures)of known attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion. Like a virus detectionsystem, it cannot detect new kinds of attacks[8].
Specification-based detection: The system defines a set of constraintsthat describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the definedconstraints.

II. INTRUSION DETECTION IN MANETS

Many intrusion detection systems have been proposed in traditional wirednetworks, where all traffic must go through switches, routers, or gateways.Hence, IDS can be added to and implemented in these devices easily [1,

7].On the other hand, MANETs do not have such devices. Moreover, the medium is wide open, so both legitimate and malicious users can access it. Furthermore, there is no clear separation between normal and unusualactivities in a mobile environment. Since nodes can move arbitrarily, falserouting information could be from a compromised node or a node that hasoutdated information[6]. Thus, the current IDS techniques on wired networkscannot be applied directly to MANETs.

2.1 Architectures for IDS in MANETs:

The network infrastructures that MANETs can be configured to are eitherat or multi-layer, depending on the applications. Therefore, the optimalIDS architecture for a MANET may depend on the network infrastructureitself [9]. In a network infrastructure, all nodes are considered equal, thus it may be suitable for applications such as virtual classrooms or conferences.On the contrary, some nodes are considered different in the multi-layered network infrastructure. Nodes may be partitioned into clusters with one clusterhead for each cluster. To communicate within the cluster, nodes can communicate directly. However, communication across the clusters must be done through the clusterhead. This infrastructure might be well suited for military applications[1,5].

Stand-alone Intrusion Detection Systems:

In this architecture, an intrusion detection system is run on each node independently to determine intrusions. Every decision made is based only on information collected at its own node, since there is no cooperation among nodes in the network. Therefore, no data is exchanged[10]. Besides, nodes in the same network do not know anything about the situation on other nodes in the network as no alert information is passed. Although this architecture is not effective due to its limitations, it may be suitable in a network where not all nodes are capable of running an IDS or have an IDS installed. This architecture is also more suitable for a network infrastructure than for multi-layered network infrastructure. Since information on each individual node might not be enough to detect intrusions, this architecture has not been chosen in most of the IDS for MANETs.

III. DISTRIBUTED AND COOPERATIVE INTRUSION DETECTION SYSTEMS

As shown in Fig. 3, the example of hierarchical WSNs consists of a base station and three clusters. In this architecture, every node belongs to only one of the clusters which are distributed geographically across the whole network. The objective of the architecture is to take advantage of cluster-based protocols in energy saving, reduced computation and data transmission redundancy. In this section, we propose an intrusion framework for information sharing which take advantage of hierarchical architecture to improve intrusion detection capability for all node participants. We assume that the WSN are configured and organized following cluster algorithms in hierarchical routing protocols. In setup phase, sensor networks are organized into clusters cluster heads are selected. Cluster heads are responsible for data fusion and computation. Once the cluster head has all the data from the nodes in cluster, it aggregates and transmits data to base station. Cluster head (denoted to CH) acts like a local base station. Sensors in cluster elect themselves to be a CH at any given time with a certain probability, more detail can be found in [13,15]. The role of being CH is not fixed by randomized rotation in a period of times. By incorporating adaptive clustering protocol, the energy spending on sensor node is equally distributed in each cluster and the amount of information transmitted to base station is reduced.

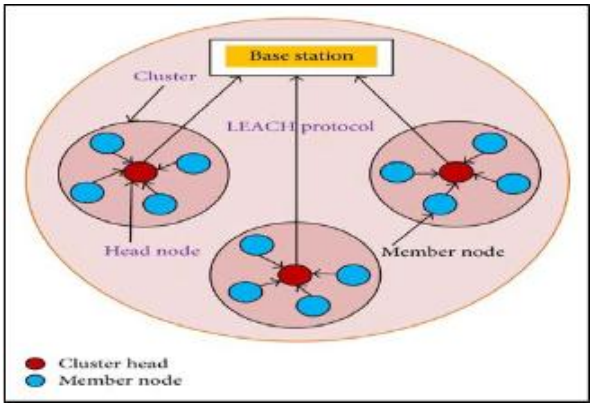

Figure 3: Hierarchical Architecture

3.1 Distributed Intrusion Detection System Using MultipleSensors:
It can be proposed a multi-sensor intrusion detection systembased on mobile agent technology. The system can be divided into threemain modules, each of which represents a mobile agent with certain functionality: monitoring, decision-making or initiating a response. By separating functional tasks into categories and assigning each task to a differentagent, the workload is distributed which is suitable for the characteristics ofMANETs[7].

3.1.1.Monitoring agent
Two functions are carried out at this class of Agent: network monitoring and host monitoring. A host-based monitor Agent hosting system-level sensors and user-activity sensors is run onevery node to monitor within the node, while a monitor agent with a network monitoring sensor is run only on some selected nodes to monitor at packet-level to capture packets going through the networkwithin its radio ranges[8].

3.1.2. Action agent
Every node also hosts this action agent. Since everynode hosts a host-based monitoring agent, it can determine if there is any suspicious or unusual activities on the host node based on anomaly detection. When there is strong evidence supporting the anomaly detected, this action agent can initiate a response, such as terminating the process or blocking a user from the network[12].

3.1.3.Decision agent
The decision agent is run only on certain nodes, mostly those nodes that run network monitoring agents. These nodes collect all packets within its radio range and analyze them to determine whether the network is under attack. Moreover, from the previous paragraph, if the local detection agent cannot make a decision on its own due to insufficient evidence, its local detection agent reports to this decision agent in order to investigate further[13]. This is done by using packet-monitoring results that comes from the network-monitoring sensor that is running locally. If the decision agent concludes that the node is malicious, the action module of the agent running on that node as described will carry out the response.

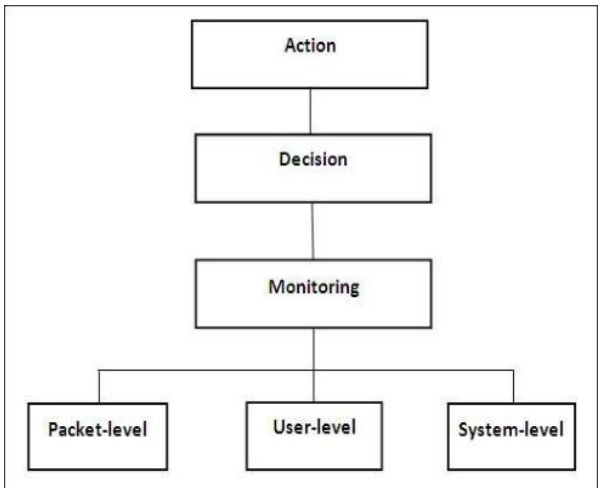

Figure 4: Network-monitoring sensor

The network is logically divided into clusters with a single clusterheadfor each cluster. This clusterhead will monitor the packets within the cluster and only packets whose originators are in the same cluster are captured and investigated. This means that the network monitoring agent (with network monitoring sensor) and the decision agent are run on the clusterhead. In this mechanism, the decision agent performs the decision-making based on its own collected information from its network-monitoring sensor; thus, other nodes have no influence on its decision. This way, spoofing attacks and false accusations can be prevented[12].

3.2 Dynamic Hierarchical Intrusion Detection:
Since nodes move arbitrarily across the network, a static hierarchy is notsuitable for such dynamic network topology. Sterne et al. [14] proposed adynamic intrusion detection hierarchy that is potentially scalable to largenetworks by using clustering .Every node has the responsibilities of monitoring (by accumulating counts and

statistics), logging, analyzing (i.e., attack signature matching or checking on packet headers and payloads), responding to intrusions detected if there is enough evidence, and alerting or reporting to clusterheads.

3.2.1.Data fusion/integration and data reduction

Clusterheads aggregate and correlate reports from members of the cluster and data oftheir own. Data reduction may be involved to avoid conflicting data,bogus data and overlapping reports. Besides, clusterheads may sendthe requests to their children for additional information in order tocorrelate reports correctly.

3.2.2. Intrusion detection computations

Since different attacks require different sets of detected data, data on a single node might not be able181to detect the attack, e.g., DDoS attack, and thus clusterheads alsoanalyze the consolidated data before passing to upper levels.

3.2.3.Security Management

The uppermost levels of the hierarchy havethe authority and responsibility for managing the detection and response capabilities of the clusters and clusterheads below them. Theymay send the signatures update, or directives and policies to alter the configurations for intrusion detection and response. These update and directives will flow from the top of the hierarchy to the bottom.To form the hierarchical structure, every node uses clustering, which is typically used in MANETs to construct routes, to self-organize into localNeighborhoods (first level clusters) and then select neighborhood representatives (clusterheads). These representatives then use clustering to organizethemselves into the second level and select the representatives. This processcontinues until all nodes in the network are part of the hierarchy. The authors also suggested criteria on selecting clusterheads. Some of these criteriaare:

Connectivity: the number of nodes within one hop

Proximity: members should be within one hop of its clusterhead.

Resistance to compromise (hardening): the probability that the nodewill not be compromised. This is very important for the upper levelclusterheads.

Processing power, storage capacity, energy remaining, bandwidthcapabilities additionally, this proposed architecture does not rely solely on promiscuous node monitoring like many proposed architectures, due to its unreliability as described in [5]. Therefore, this architecture also supports directperiodic reporting where packet counts and statistics are sent to monitoringnodes periodically.

3.3 Intrusion Detection Techniques for Node Cooperation in MANETs:

Since there is no infrastructure in mobile ad hoc networks, each node mustrely on other nodes for cooperation in routing and forwarding packets to thedestination. Intermediate nodes might agree to forward the packets but actually drop or modify them because they are misbehaving. The simulationsin [5] show that only a few misbehaving nodes can degrade the performanceof the entire system. There are several proposed techniques and protocolsto detect such misbehavior in order to avoid those nodes.

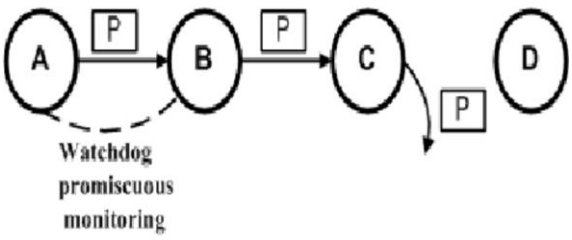

Figure 5: How watchdog works: Although node B intends to transmit apacket to node C, node A could overhear this transmission

IV. SUMMARY OF IDS FOR DETECTING MISBEHAVING NODES

Although the watchdog is used in all of the above IDS, but there are several limitations. The watchdog cannot workproperly in the presence of collisions, which could lead to false accusations. Moreover, when each node has different transmission ranges or implementsdirectional antennas, the watchdog could not monitor the neighborhood

accurately.All of the above IDS's presented are common in detecting selfish nodes.However, CORE doesn't detect malicious misbehaviors while the others detect some of them, i.e., unusually frequent route update, modifying headeror payload of packets, no report of failed attempts, etc.

V. CONCLUSIONS AND FUTURE DIRECTIONS

An intrusion detection system aims to detect attacks on mobile nodesor intrusions into the networks. However, attackers may try to attack theIDS system itself. Accordingly, the study of the defense to such attacksshould be explored as well.Many researchers are currently occupied in applying game theory forcooperation of nodes in MANETs as nodes in the networkrepresent some characteristics similar to social behavior of human in a community. That is, a node tries to maximize its benefit by choosing whetherto cooperate in the network. There is not much work done in this area,therefore, it is an interesting topic for future research.

VI. REFERENCE

[1] Y. Zhang, W. Lee, and Y. Huang, Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal(ACM WINET), Vol. 9, No. 5, September 2003.
[2] A. Mishra, K. Nadkarni, and A. Patcha, \Intrusion Detection in Wire-less Ad Hoc Networks," IEEE Wireless Communications, Vol. 11, Issue1, pp. 48-60, February 2004.
[3] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, \Security in AdHocNetworks: a General Intrusion Detection ArchitectureEnhancing Trust Based Approaches," Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002), pp. 1-12, April 2002.
[4] O. Kachirski and R. Guha, \E®ectiveIntrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks," Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03),p. 57.1, January 2003.
[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, \Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proceedings of the 6th AnnualInternational Conference on Mobile Computing and Networking (MobiCom'00), pp. 255-265, August 2000.
[6] D. B. Johnson, and D. A. Maltz, \The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (Internet-Draft)," Mobile Ad-hocNetwork (MANET) Working Group, IETF, October 1999.
[7] P. Brutch and C. Ko, \Challenges in Intrusion Detection for WirelessAd-hoc Networks," Proceedings of 2003 Symposium on Applications andthe Internet Workshop, pp. 368-373, January 2003.
[8] Y. Huang and W. Lee, \A Cooperative Intrusion Detection System forAd Hoc Networks," Proceedings of the ACM Workshop on Security inAd Hoc and Sensor Networks (SASN'03), pp. 135-147, October 2003.
[9] P. Michiardi and R. Molva, \A Game Theoretical Approach to EvaluateCooperation Enforcement Mechanisms in Mobile Ad Hoc Networks,"Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks(WiOpt'03), March 2003.
[10] A.Agah, S. K. Das, K. Basu, and M. Asadi, \Intrusion Detection inSensor Networks: A Non-Cooperative Game Approach," Proceedingsof the 3rd IEEE International Symposium on Network Computing andApplications (NCA'04), pp. 343-346, 2004.
[11] Ilyas, M., Mahgoub, I.: Handbook of sensor networks: Compact wireless and wired sensing systems. CRC Press, Boca Raton, USA (2005)
[12] Wood, A.D., Stankovic, J.A.: Denial of Service in Sensor Networks. Computer 35(10),54–62 (2002)
[13] Karlof, C., Wagner, D.: Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Elsevier's Ad. Hoc. Networks Journal, Special issue on sensor network applications and protocols (2003)
[14] Djenouri, D., Khelladi, L., Badache, A.N.: A survey of security issues in mobile ad hoc and sensor networks. Communications Surveys & Tutorials 7(4), 2–28
[15] Heady, R., et al.: The Architecture of a Network Level Intrusion Detection System. Computer Science Department, University of New Mexico, Tech. Rep. (August 1990)