Distributed Intrusion Detection Architecture Based on Clustering of the Nodes that Addresses the Security Vulnerabilities of the Ad-hoc networks

Nelli Chandrakala [1] **Chelloju Raju [2]**

[1,2] Assistant Professor in CSE, Christu Jyothi institute of Technology & Science, Jangaon

Abstract-Intrusion detection in wireless ad hoc networks is a challenging task because these networks change their topologies dynamically, lack concentration points where aggregated traffic can be analyzed, utilize infrastructure protocols that are susceptible to manipulation, and rely on noisy, intermittent wireless communications. Security remains a major challenge for these networks due their features of open medium, dynamically changing topologies, reliance on cooperative algorithms, absence of centralized monitoring points, and lack of clear lines of defense. In this paper, we present a cooperative, distributed intrusion detection architecture based on clustering of the nodes that addresses the security vulnerabilities of the network and facilitates accurate detection of attacks. The architecture is organized as a dynamic hierarchy in which the intrusion data is acquired by the nodes and is incrementally aggregated, reduced in volume and analyzed as it flows upwards to the cluster-head. The cluster heads of adjacent clusters communicate with each other in case of cooperative intrusion detection. For intrusion related message communication, mobile agents are used for their efficiency in lightweight computation and suitability in cooperative intrusion **detection.**

Keywords: intrusion detection, wireless ad hoc networks, security, denial of service attack.

I. Introduction

A wireless ad hoc network consists of a collection of mobile nodes that communicate with each other through wireless links without the aid of any pre-existing communication infrastructure. Nodes within each other's radio range communicate directly via wireless links, while those that are far apart rely on intermediate nodes to forward their messages. Each node can function as a router as well as a host. Unlike fixed wired networks, wireless ad hoc networks have many operational limitations. For example, the wireless links are constrained by transmission range and bandwidth, and the mobile nodes may have limited battery life, CPU processing power, and memory. The network topology may change rapidly due to mobility of the nodes, and continuous joining and leaving of the nodes in the network. While these characteristics make ad hoc networks more flexible, they introduce security concerns that are either absent or less severe in wired networks. Ad hoc networks are vulnerable to various kinds of attacks that include passive eavesdropping, active interfering, impersonation, and denial of service. Although, intrusion prevention measures such as strong authentication and redundant transmission can be used to improve the security of these networks, these techniques can address only a subset of the threats and they are very costly to implement.

The dynamic nature of ad hoc networks requires that prevention techniques should be complemented by detection techniques to monitor security status of the network and identify any malicious behavior [1]. Intrusion detection is a second line of defense that provides local security to a node, and also helps in establishing a specific *trust level* of a node in an ad hoc network [2]. Since it is impossible to adopt a fully centralized approach to security in ad hoc networks [3], a cluster-based semi-centralized approach may be adopted that helps in integration of local intrusion detection in a node or in a cluster with network-wide global intrusion detection. In this paper, we propose an architecture of a cluster based intrusion detection system for wireless ad hoc networks. In the proposed scheme, an ad hoc network is divided into different clusters using a suitable clustering algorithm [4]. The clustering makes the communication between the nodes in the network more efficient, as each cluster is managed by its cluster-head and inter-cluster communication takes place only through the gateway nodes [5]. The task of cluster management in a cluster is delegated to the cluster-head, which is chosen based on the output an election algorithm that is invoked periodically. The rotation of cluster management responsibility to different nodes ensures a proper load balancing and fault-tolerance in the system [6]. We propose to delegate the cluster-wide intrusion detection responsibility to the cluster-heads, as apart from their default function of cluster management, they can initiate a cooperative approach for intrusion detection. Every node in the network maintains a database of known attacks (misuse signatures). Anomalous activities are defined in terms of upper and lower thresholds for identifying any new attack against the network [7]. The use of mobile agents is proposed for inter-cluster communication. The mobile agents are light-weight and computationally efficient small software components. They enhance the flexibility in cooperative detection ability of a distributed intrusion detection system [8]. However, there have been some ecurity concerns about the mobile agents which need to be investigated further [9][10].

II. Related Work

In a cooperative distributed intrusion detection system proposed by Zhang and Lee [1], every node in an ad hoc network analyzes locally available network data for anomalies. Intrusion attempts are detected by employing a distributed cooperative mechanism. Each node runs intrusion detection agents consisting of six modules. The model uses multi-layer integration approach to analyze the attack scenario. However, the scheme requires large amount of data that needs to be passed over wireless links to update the local database of anomaly and misuse rules. This is certainly a problem in low bandwidth wireless links. Another issue that needs to be addressed is how to obtain enough audit data to establish the normal patterns of users. Without this data, it is almost impossible to carry out anomaly detection accurately. Li et al. [2] have used mobile agents for developing a coordinated distributed intrusion detection scheme for ad hoc networks. In the proposed scheme, the mobile nodes are divided into different clusters. The cluster-heads act as the manager nodes that contain *assistant mobile agents* and *response mobile agents*. Each cluster-member node (nodes other than the cluster-heads) runs a *host monitor agent* to detect network and host intrusions using *intrusion analyzer* and *interpretation base*. The assistant agent running on a cluster-head is responsible for collecting intrusion-related data from the cluster-member nodes. The response agent on a cluster-head informs the cluster-member nodes about any response initiated by the intrusion detection system against

possible intrusive activity on the network. However, the architecture is not modular as there is no separation of functions between the cluster-head nodes and cluster-member nodes. Moreover, it does not use any clustering algorithm to minimize message communication in the network for intrusion detection and response. Kachriski and Guha [3] have presented an intrusion detection system for ad hoc networks, in which multiple sensors deployed throughout the network collect and merge audit data implementing a cooperative detection algorithm. Sensors are deployed on some of the hosts in the network that monitor the network traffic. The selection of these nodes is based on their connectivity index and the outcome of a distributed voting algorithm. The detection decisions are taken by mobile agents that transport their execution and state information between different sensor hosts of the network, and finally return to the originator host with the result. The authors have proposed two different methods of decision making: independent and collaborative. The approach of independent decision making by mobile agents is susceptible to single point of failure, and therefore, the authors have recommended the use of collaborative approach. The main advantage of this proposition is the restriction of the computation-intensive operations of the system to a few dynamically elected nodes. However, since the mobile agent platforms are themselves vulnerable, the security proposed scheme may be questionable [10]. Albers et al. have proposed a distributed and collaborative architecture of intrusion detection system by using mobile agents [5]. The authors have proposed the use of a local intrusion detection system (LIDS) for monitoring the local activities on each node. Two types of data are exchanged among the LIDS: security data and intrusion alerts. LIDS agents use either the anomaly or misuse detection. Once a local intrusion is detected, the LIDS initiates a response and informs other nodes in the network. Upon receiving an alert, the LIDS protects itself against intrusion by use of a suitable defense mechanism. Sun et al. have presented an architecture of a *zone-based intrusion detection system* (ZBIDS) that involves a local detection and a collaborative detection technique [12]. The local detection module consists of a general intrusion detection agent model and a Markov chain-based anomaly detection algorithm. To enhance the detection efficiency, the collaborative detection module is utilized. The collaborative detection module works on the ZBIDS agents and uses an aggregation algorithm on the gateway nodes in the clustered ad hoc network. The authors have proposed the IDS for securing routing in the network. The simulation results demonstrate that the proposed scheme is not only efficient in detecting intrusions but also it has reduced false alarm rates appreciably. Sterne et al. have proposed a dynamic intrusion detection hierarchy that is potentially scalable to large networks [13]. The mechanism is based on a clustering approach, in which the nodes may be organized in a hierarchy with the cluster-head nodes at the top level of the hierarchy. Every node in the network monitors, logs, analyzes, and sends alerts, and responds to the alerts send by other nodes. The cluster heads have the additional tasks of (i) data filtering and data fusion, (ii) detection of intrusions and (iii) security management. Wang et al. have proposed an end-to-end detection of wormhole attack (EDWA) that is based on a set of mechanisms [14]. In wormhole attack, an adversary builds a tunnel between two end points which are multiple hops way from each other. The message recorded at one is relayed to the other end from where it is broadcasted into the network again. In the proposed defense mechanism against wormhole attack, the authors have proposed a location-based detection mechanism where the source node estimates the minimum hop count to the destination based on the geographic information of the two end hosts in which the receiver's location is piggy-backed by the route reply packet during the route discovery. For, a received route, the source compares the

hop count value received from the reply packet with its estimated value. If the received value is less than the estimation, the corresponding route is marked as if a wormhole is detected. The, the source launches wormhole *tracing* in which the two end points of the wormhole will be identified in a small area provided that there are multi-paths existing between the source and destination. Finally, a normal route is selected for data communication.

III. Proposed Architecture

Cooperative intrusion Detection Architecture

This section proposes a cooperative intrusion detection architecture for the MANET environment described above. How the dynamic hierarchy facilitates cooperative intrusion detection. Construction of the hierarchy using attribute-based . Two additional topics relating to the utilization of the hierarchy are discussed describes the responsibilities of nodes according to their placement within the hierarchy.

Organizational model: a dynamic hierarchy

The choice of an organizational model is fundamental to the architecture of any distributed system. Common models include static hierarchy, peer-to-peer (P2P) and publish-and-subscribe. The static nature of the static hierarchy model, the potentially huge volume of multi-hop traffic that may be generated as a result of the arbitrary transfer of information in the P2P and publish and subscribe models as well as assumptions of uniform trust in P2P models render them inappropriate for our problem domain. In order to provide incremental aggregation, detection, and correlation, efficient dissemination of intrusion management directives, and scalability, the organizational model we propose is the dynamic hierarchy. The major advantage of a hierarchy is its potential scalability to large networks, since it can provide rapid and communications-efficient detection for local cooperative attack recognition, while still allowing data sharing for more widely-distributed cooperative intrusion detection algorithms. Unlike P2P networks where communications overhead can rise by the square of the number of nodes, a hierarchical approach allows higher-layer nodes to selectively aggregate and reduce intrusion detection data as it is reported upward from the leaf nodes to a root. Moreover, a hierarchy naturally aligns with the authority structure or chain-of-command that is common to many human organizations and governs the control of assets, in this case, network nodes and services. In the proposed architecture, this structure is represented by the flow of data to authoritative nodes at the root of the hierarchy, which dispatch directives down to lower levels. In this problem domain, mobility and other factors will cause the topology to change continually, such that an initially-defined static hierarchy will soon be inefficient. Since both nodes and links will appear and disappear rapidly and normally, a dynamic, topology based hierarchy must be formed and constantly maintained. Nodes will communicate intrusion detection information most often with other nodes that are their parents or children in the hierarchy. Efficiency will generally be improved if a significant fraction of children are topologically nearby, such as being link-layer (1-hop) neighbors. Since mobility and other factors will lead to frequent changes in these topological relationships, hierarchical relationships between nodes need to evolve as the topology evolves. We propose to use *clustering* [1,4,5] for establishing and maintaining such a dynamic evolving hierarchy of intrusion detection components. An example of this infrastructure is nodes annotated with a “1” are the representatives of first level clusters. Arrows pointing to these nodes originate from the other

(leaf) nodes in their cluster that report to them. Similarly, arrows from first level representatives to their second level representative (annotated with a "2"), show the composition of one of the second level clusters. The arrow from the second level representative to the third level representative shows that the former is a member of a third level cluster; other members of that cluster are outside the scope of the figure and are not shown. To avoid having a single representative node at the top of the hierarchy that is a potential single point of failure, one or more members of the highest level cluster should be designated as backup representatives. This infrastructure allows intrusion detection observations to be gathered efficiently from the entire network; provides incremental aggregation, detection, and correlation; and efficient dissemination of intrusion response and management directives (e.g., signature updates).

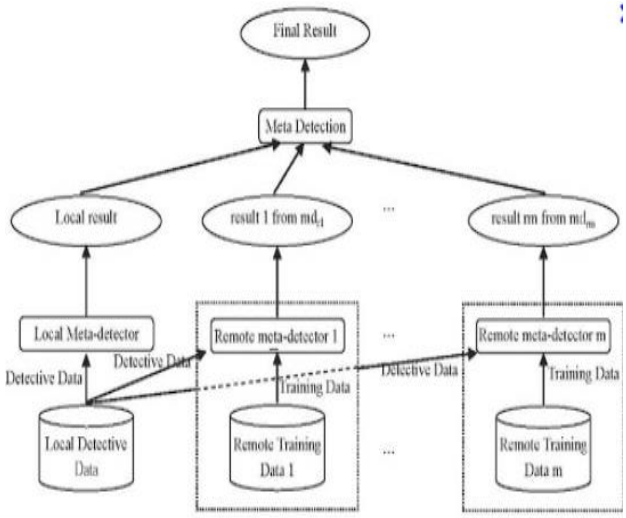

Fig1**. Co-Operative Distributed intrusion Architecture.**

Dynamic hierarchy for Intrusion Detection

In the proposed architecture, every node is responsible for using its own resident network and host-based intrusion detection mechanisms to protect itself. In addition, nodes are assigned intrusion detection responsibilities to help protect other nodes in the network. These responsibilities include monitoring, logging, analyzing, and reporting network data at various protocol layers. The responsibilities of a node depend on its current positions in the topology and the dynamic hierarchy. Nevertheless, data acquisition will generally occur at or near the bottom of the hierarchy where leaf nodes are attached. Intrusion detection data of all forms including alerts will generally flow upward and will be consolidated, correlated, and summarized incrementally as it flows upward. A small collection of nodes at the uppermost levels of the hierarchy will serve as security management nodes that may possess an integrated view of the overall cyber security of the network. These nodes will also provide facilities for sending directives to all the nodes in the network, such as directives to alter all nodes' intrusion detection or intrusion response configurations; these will flow down the hierarchy from top to bottom. In short, data from intrusion detection systems needs to flow from the bottom to the top where it can be utilized in decision-making. Once decisions are made, they are transformed into directives that flow from the top to the bottom. Different kinds of attacks require different sets of

detection data, and this data may aggregate at different levels in the hierarchy. A key principle is that intrusion detection and correlation should occur at the lowest level in the hierarchy at which the aggregated data is sufficient to enable an accurate detection or correlation decision. If the data available at a level is not sufficient, it is pushed upward in the hierarchy where it is further aggregated with other data. One reason for this principle is *detection latency* – in the absence of a suspicious event, data will generally be reported periodically by group members to their cluster head. If a member possesses sufficient data to make an immediate detection decision, but defers detection processing to its next-level representative and only transfers the data to the parent periodically, this will introduce a delay in detecting an attack. Another reason is that performing intrusion detection is a form of *data reduction* in which concise inferences are drawn from potentially large amounts of data. If a node performs intrusion detection on a set of data, it may free itself from having to transmit the entire data set to its representative; instead, if an attack is detected, the node may only need to send an alert and the associated, relevant evidence. The dynamic intrusion detection hierarchy provides a scalable and efficient structure for organizing intrusion detection components. Nevertheless, there will be situations in which information may need to flow outside this structure, i.e., it may need to flow directly between components that are neither peers nor hierarchically related. Hence, other styles of communication are also supported. Topological clustering, which is typically used in MANETs to construct routes, permits the creation of a logical hierarchy that can adjust to topology changes on the fly. Cluster-head selection occurs at many levels. Peer nodes use clustering to self-organize into local neighborhoods (first level clusters) each of which selects a neighborhood representative i.e., cluster-head. These representatives then use clustering to organize themselves into second level (regional) clusters. These clusters select representatives, which then organize themselves into third level clusters, and so forth until all the nodes in the network are interconnected by a hierarchy of representatives, with a small cluster at the top. The bandwidth efficiency of such an architecture depends on exploiting topological characteristics to organize nodes into groups. However, a mixture of topological and other criteria are used to select cluster-heads. Some of these criteria, which may be used only at particular levels in the hierarchy, include connectivity, proximity, resistance to compromise, accessibility by network security specialists, processing power, storage capacity, energy remaining, bandwidth capabilities, and administratively designated properties. Connectivity is the measure of how many other nodes a given node can talk to directly. Proximity is particularly important for organizing the lowest level groups; each member should be within one hop of its representative. This restriction provides resilience by ensuring that an initial level of cooperative exchange among neighboring detectors can occur without any reliance on MANET routing, which may be targeted by an adversary and disabled or compromised. In other words, communication within first level groups can function even when routing services are not available. In addition, since single-hop communications are significantly more efficient than multi-hop communications, this approach provides high communications efficiency for a significant fraction of the overall set of communication paths within the cooperative hierarchy. Resistance to compromise (hardening) is an administratively-designated attribute that describes the probability that the node will not fall into adversarial control. Selection of upper level cluster-heads is weighted more heavily to emphasize resistance to compromise. The organization may also allow a roving security management node to take top priority in the hierarchy or allow the hierarchy to tie into a static security management network if available. However, if neither is available, the hierarchy

should generally attempt to find alternatives among the nodes that are available and meet minimum requirements. Since the operation of some MANETs will be overseen by one or more network security specialists, nodes used by such specialists as security management consoles will typically assume positions at the top of the hierarchy. Processing power and storage capacity are additional attributes describing the ability of the node to perform computation and retain data. Energy remaining is either the measure of battery power left, or indication of an externally powered node (i.e., part of a fuel-powered vehicle). Bandwidth capabilities indicate the node's potential network throughput, and may vary greatly across different hardware platforms. Administratively designated properties include any additional attributes of the nodes that may be relevant.

IV. Performance Analysis

The proposed scheme has been implemented on network simulator *ns-2* [15] to evaluate its performance. The 802.11 MAC layer in ns2 is used for this purpose. The chosen parameters for simulation are shown in Table I. Before we discuss the performance results of the system, we describe the simulation for clustering. For cluster formation in the network, we have simulated *passive clustering*. Passive clustering is an on-demand protocol. It constructs and maintains the cluster architecture only when there are on-going data packets that piggyback cluster-related information (e.g. the state of a node in a cluster, the IP address of the node etc.). Each node collects neighbor information through promiscuous packet receptions. Passive clustering has also two essential components: (i) first declaration wins rule and (ii) gateway selection heuristic. With the *first declaration wins rule*, a node that first claims to be a cluster-head, rules the rest of the nodes in its cluster area. Each cluster is assumed to be 2-hop long, i.e., each cluster-member may be at a maximum 2-hop distance from its cluster-head. In passive clustering, to make sure that all the neighbors have been checked, there is no waiting period. This is in contrast to all the weight-driven clustering mechanisms [4]. The cluster-heads are assumed to broadcast their beacons over 2 hops in every 20 seconds time interval. The *gateway selection heuristic* provides a procedure to elect the minimum number of gateways (including distributed gateways) required to maintain the connectivity in a distributed manner. A gateway is a bridge node that connects two adjacent clusters. The beacon message, sent periodically by a cluster-head in a cluster, contains information that includes the identifications of the cluster-members, and the gateway node in the cluster. The gateway nodes also send beacons to inform the cluster-members about the adjacent clusters. In the proposed scheme, the gateway selection mechanism is designed in such a way that it eventually allows only one gateway for each pair of neighboring cluster-heads. However, in certain situations it may be possible that there is no gateway node between two clusters. This scenario, although very unlikely in reasonably dense ad hoc networks, may occur if two adjacent cluster heads are mutually reachable not by a two-hop route. Then the clustering scheme should select the two intermediate nodes as distributed gateways. Passive clustering maintains clusters using implicit time-out. A node assumes that the nodes it had previously heard from have died or are out of its locality if they have not sent any data within the time-out duration. With a reasonable network communication load, a node can easily keep track of dynamic topology changes by virtue of this time-out. For the purpose of evaluation of the detection efficiency of the system, we have simulated four types of attacks on the network layer. We have assumed that the goal of the attacker is to degrade the performance of the network or individual nodes instead of gaining privileges of

a particular node in the network. This assumption means that the proposed IDS focuses on detecting traffic-related attacks. Some of the well known attacks in this category are: power exhaustion, storage and CPU exhaustion attacks, network bandwidth exhaustion attacks such as flooding and deprivation attacks, routing-disruption attacks such as black-hole and gray-hole attacks etc. [16]. Table II shows the experimental results obtained from the simulation. It is observed that the proposed system have effectively detected the simulated attacks launched against it at the network layer with a very low false positive rates. More sophisticated attack simulations at transport and application layer will be made and results will be reported when available.

Table.I

Attack Type	Detection Rate	False Alarm Rate
Flooding	100%	2.8%
Blackhole	99.3%	0.3%
Sleep Deprivation	90%	0.7%
Packet Dropping (All)	93%	0.5%

V. Conclusion

In this paper, we have presented a Co-Operative Distributed intrusion detection architecture for wireless ad hoc networks. The clustering of the network nodes makes message communication efficient and intrusion detection system robust. Local detection allows for detection of attacks, which are localized to a node or a cluster, whereas global detection involves collaboration among the nodes in different clusters. A mobile agent framework is deployed for communication among the nodes for intrusion related information. The results obtained in simulations show that the scheme is effective and efficient. As a future scope of work, we plan to identify different attack techniques and their consequences at different layers of the TCP/IP stack. We also plan to investigate and determine the optimum number of clusters that maximizes the system performance.

REFERENCES

[1] X. Wang, J.Wong. “An end-to-end detection of wormhole attack in wireless ad hoc networks”, Proc. of 31st Annual International Computer Software amd Applications Conference (COMPSAC ’07), pp. 39-48, Beijing, China, July 2007Y. [2] S. Buchegger, J.L. Boudec, “Performance analysis of the CONFIDANT protocol: cooperation of nodes- fairness in dynamic ad-hoc networks,” Proc. of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc’02), June 2002, pp. 226-236.

[3] Sun, K. Wu, U.W. Pooch. “Zone-based Intrusion Detection for Mobile Ad Hoc Networks. Ad Hoc and Sensor Wireless Networks”, Vol 2, No. 3, 2006.

[4] C.R. Lin, M. Gerla, “Adaptive clustering for mobile wireless networks” *IEEE Journal on Selected Areas in Communications*, Vol. 15, No. 7, September 1997, pp. 1265-1275.

[5] L. Ramachandran, M. Kappor, A. Sarkar and A. Aggarwal, "Clustering algorithms for wireless ad hoc networks", Proc. of the 4th International Workshop on Discrete Algorithms and Methods fr Mobile Computing and Communications, pp. 54-63, USA 2000.

[6] S. Banerjee, S. Khullar, "A clustering scheme for hierarchical control in wireless networks", Proc. of the IEEE INFOCOM, 2001

[7] A.B. Smith, "An examination of an intrusion detection architecture for wireless ad hoc networks", Proc. of the National Colloquium for Information Systems Security Education, May 2001.

[8] O. Kachirski, R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks", Proc. of the 36th Hawaii International Conference on System Sciences (HICSS'03), IEEE, 2002.

[9] J.E. White. "Telescript Technology Mobile Agents." General Magic White Papers, 1996.

[10] W. Farmer, J.Guttman, and V. Swarup. "Security for Mobile Agents: Authentication and State Appraisal", Proc. of the European Symposium on Research in Computer Security (ESORICS), LNCS, September 1996.

[11] Li, C., Song, Q., and Zhang, C. "MA-IDS architecture for distributed intrusion detection using mobile agents", Proc. of the 2nd International Conference on Information Technology (ICITA), 2004.

[12] P. Albers, O. Camp, J-M. Percher, B. Jouga, M. Ludovic, and R. Puttini, "Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches", Proc. of the First International Workshop on Wireless Information Systems (WIS- 2002), April 2002, pp.1-12.

[13] D.Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R.Talpade C.Ko, R. Balupari, C-Y. Tseng, T. Bowen, K. Levitt, J. Rowe, "A General Cooperative Intrusion DetectioN Architecture for MANETs", In Proc. of the 3rd IEEE International Workshop on Information Assurance, pp. 57-70, 2005.

[14] Y. Zhang, W. Lee, "Intrusion detection in wireless ad-hoc networks," Proc. of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM'2000), pp. 275-283, Aug 6- 11.

.

[15] NS-2 Simulator. URL: http://www.isi.edu/nsnam/ns.

[16] Y.-C. Hu, A. Perrig, "A survey of secure wireless ad hoc routing", IEEE Security and Privacy Magazine, Vol. 2, No. 3, pp. 28-39, May-
June 2004