ICIC Express Letters
Part B: Applications
Volume **10**, Number **9**, September **2019**

ICIC International ©2019 ISSN 2185-2766
pp. **813–821**

DYNAMIC INTRUSION DETECTION TECHNIQUE FOR DYNAMIC MOBILE AD HOC NETWORK

Farhan Abdel-Fattah[1], Khalid Abdul-Fattah Farhan[1]
Feras Hamed Al-Tarawneh[1] and Ali Mahmoud Al-Naimat[2]

[1]Faculty of Science and Information Technology
Al-Zaytoonah University of Jordan
P.O. Box 130, Amman 11733, Jordan
{ Farahan.A; Khalid.F; F.altarawneh }@zuj.edu.jo

[2]Faculty of Information Technology
The World Islamic Sciences and Education University
Tabarbour, P.O. Box 1101, Amman 11947, Jordan
Ali.naimat@wise.edu.jo

Received February 2019; accepted May 2019

Abstract. *In this paper, we present the architecture and operation of a dynamic agent-based intrusion detection technique in Mobile Ad Hoc Network (MANET). The proposed technique has cooperative agents' architecture. Traditional intrusion detection techniques have trouble dealing with dynamic environments such as collecting real-time attack related audit data and cooperative global detection. The proposed detection technique comprises a set of static and mobile agents. Autonomous agents can perform specific intrusion detection tasks which are used to collect data, detect intrusions, distribute aggregated intrusion information to all other mobile nodes in MANET in an intelligent way, and collaborate with other agents.*
Keywords: Network security, Ad hoc network, Intrusion detection, Multi agent system, MANET, IDS

1. **Introduction.** The Mobile Ad Hoc Network (MANET) consists of nodes which are built up from mobile and dynamic devices such as laptops and smart phones. These devices communicate with each other using atmosphere and set up a temporary dynamic network without any help of fixed infrastructure or a centralized administration. The absence of a centralized administration and node mobility makes the MANETs' nodes to be all to serve as both hosts and routers. So security is the main challenge in MANET [1-3]. In general, the cooperation of all nodes in MANET ensures reliable routing services. On the other hand, dependency and decentralization of MANET allows an adversary to exploit new types of attacks that are designed to destroy the cooperative algorithms used in ad hoc networks. Moreover, due to their open medium, dynamically changing network topology and lacking central monitoring and absence of a clear line of defense, MANET is particularly vulnerable to several types of attacks like passive eavesdropping, active impersonation, and denial of services. An intruder that compromises a mobile node in MANET can destroy the communication between the nodes by broadcasting false routing information, providing incorrect link state information, also overflowing other nodes with unnecessary routing traffic information [4]. Therefore, successful implementation of mobile ad hoc network will depend on users' confidence in its security. The security research in MANET focused on key management, routing protocol and intrusion detection techniques [5]. However, past experiments have shown that encryption and authentication as intrusion prevention are not sufficient [1]. At present, completely preventing breaches

DOI: 10.24507/icicelb.10.09.813

of security seems unrealistic, especially in cellular Internet, wireless and mobile ad hoc network [4,6]. On the other hand, intrusion detection techniques used in wired networks cannot be directly applied to mobile ad hoc networks due to special characteristics of the networks.

In MANETs, it is very difficult for an intrusion detection technique to make decision just based on data collected locally. Nodes must collaborate or exchange in making an intrusion detection decision. Therefore, the proposed intrusion detection models should support the cooperation and collaborations between nodes. Multi agent system is an emerging technology that provides cooperation and collaboration [7]. Thus, in this paper the technology is utilized for the process of making intrusion detection decision. In this work intrusion detection architecture is proposed based on regions. The model consists of two layers: region member layer and gateway layer. The whole network is logically divided into several regions, and each of them consists of one or more special nodes as the gateway nodes and several normal nodes as the region members nodes. Our proposed architecture seeks to detect intrusive behavior by identifying and analyzing network parameters that deviate from an expected behavior during an attack. This paper is organized as follows. In Section 2, related work in the area of intrusion detection is presented. Section 3 presents the agent-based intrusion detection methodology and architecture, and the simulation and implementation are discussed in Section 4. Finally, Section 5 gives conclusion.

2. **Related Work.**

2.1. **Intrusion detection mechanism.** Intrusion detection is a security mechanism that tries to recognize unauthorized (not legitimate) individuals (outside threat) who are attempting to break into or compromise and misuse a system, also, those who have legitimate access to the system (inside threat), but misuse and abuse their privileges [1,8]. Moreover, the intrusion detection system is a computer security tool that always monitors the system and user activity in the network and computer systems, in order to detect unauthorized access. Therefore, Intrusion Detection System (IDS) is designed to discover malicious activities that try to compromise the confidentiality, integrity and assurance of computer systems [2,9-11]. If the intrusion is detected, a response can be directly initiated to prevent or to limit the damages to the system. However, the essential aim of any intrusion detection is to catch doers in the act before they do any real damage to your systems and resources.

2.2. **Architectures for intrusion detection in MANET.** The intrusion detection mechanism for MANET proposed by Zhang and Lee [1] in 2000, was the first discussion about the intrusion detection techniques in the MANET. This model uses distributed and cooperative decision making with anomaly detection. In this technique, local intrusion detection runs on all nodes in MANET and observes machine local activities, at the same time, it is responsible for detecting and collecting local data to recognize potential intrusions. All nodes in this model work as one group. The communication between nodes is completed via network messages. This model is appropriate for a flat ad hoc network. Hierarchical intrusion detection architecture was proposed by Huang and Lee [13]. This model extends the distributed and cooperative IDS proposed by [1]. In this model, the network is divided into clusters. A clusterhead is elected by a collection of nodes in a neighborhood or citizen nodes. The efficiency of ad hoc network is improved by limiting the usage of the resources for intrusion detection system purposes to a small number of mobile nodes. A multi-sensor intrusion detection system based on mobile agent was proposed by Kachirski and Guha [7]. The intrusion system is composed of three major models: monitoring, decision-making and action agent (response agent). The ad hoc network is divided into clusters; each cluster has only one clusterhead. The workload is distributed by dividing IDS tasks into classes and assigning each task to a different agent.

Nakeeran et al. [14] have proposed an agent-based IDS architecture that uses agents and anomaly data mining techniques for detection of intrusion. Patrick et al. [15] proposed a distributed and collaborative architecture for MANET intrusion detection system, using mobile agent technology. In this architecture, each node runs a local IDS for local concern. Each IDS detects intrusion on its node and uses external information that is derived from other Local Intrusion Detection System (LIDS) on additional machines to confirm the detection. Cooperative, distributed intrusion detection architecture was proposed by Sterne et al. [16]. The proposed intrusion system is using clustering like those in [8,13]. However, it can be organized in more than two levels. Mobile nodes of the first level of the cluster are called leaf nodes. Every node in charge of monitoring, analyzing and responding to detected intrusions if there is strong evidence, or reporting to clusterheads if the evidence is not strong enough. Cooperative intrusion detection architecture was proposed by Kominos and Douligeris [17] that incorporates a multi-layered detection approach in order for detection of malicious behaviors. In this cooperative intrusion detection architecture, three modules are installed on every node: collection module for collecting audit data; a detection module for anomaly detection; and an alert module for raising an alarm. Anomaly detection system proposed by Bose et al. [18] provides security for three layers: application layer detection engine, routing layer detection engine, MAC layer detection engine. The data of normal profile to detect intruder node is obtained from feature vectors of the training dataset. A specification-based intrusion detection system for AODV was proposed by Tseng et al. [19]. The normal behavior for important features in the ad hoc network is constructed in the first stage. Then the actual activity of the system is compared to the profiles of normal behavior of systems. This model uses Network Monitor (NM), cooperative network monitors architecture to trace the request-reply RREP flow in the MANET routing protocol. The network monitor performs all IDS functionality, and listens to wireless media to monitor AODV packets and exchange data. This architecture has a low efficiency because the packet is checked at each hop. Pattanayak and Rath [20] proposed clusters based intrusion detection and prevention architecture using mobile agent for MANET. In this architecture, a mobile agent resides in each cluster of MANET and each cluster runs a specific application at any point of time.

2.3. **Multi agent systems.** Actually, multi agent systems technology is viewed as one of the fastest growing areas of research and new applications in artificial intelligent and distributed systems. Distributed artificial intelligence concept is a group of agents; each agent cooperates and communicates with other agents in distributed environments. The concept of multi agents is a natural extension of the idea of processes in conventional operating systems. In the context of distributed systems, multi agents are autonomous processes deployed at different nodes to achieve some specific tasks. The multi agent system platforms are in charge for all the operations of agents, such as, creation, communication, migration, cloning, security and termination. If the mobility feature is added to agent, it makes him mobile. Mobile agents are special kinds of software agents, which have the ability to move through large networks. Mobile agents have been used in several techniques for intrusion detection systems in MANETs. Due to its ability to travel through the large network, each mobile agent is assigned to only one specific task. Then one or more mobile agents are distributed into each MANET's node [10,21]. This allows the distribution of the intrusion detection tasks. Through travel, the agents can interact and cooperate with nodes, collect information, and perform tasks assigned to them. Opposed to traditional approaches where large amounts of data are transported towards the computation location, it allows the analysis programs to move closer to the audit data. While providing a flexible way of distribution using mobile agents can reduce the amount of data traveled through the network. Moreover, any node dispatching an agent does not

have to wait for it to return to resume the processing; any agent can be dispatched and even destroyed by other nodes, without having to go back to the creator node [3,10,12]. The execution of the mobile code can be stopped but not terminate and resume at the next node, where the mobile agent migrates. MANETs have limited battery life, and their intermittent connections have low bandwidth, and high latency. Mobile agent techniques can overcome all these problems [20].

3. **Dynamic Intrusion Detection Architecture.** Dynamic intrusion detection is a distributed detection method, in which two levels of hierarchical structure are defined; it is designed using region-based framework. The whole network is divided into non overlapping regions shown in Figure 1. It is assumed that the existence of such a framework; this could be done without difficulty based on techniques such as geographic partitioning [3,10]. There are two categories of nodes in our model: *region member* nodes and *gateway* nodes. The node is called a gateway if it has a connection to a node in the neighboring region; otherwise, it is called a region node.

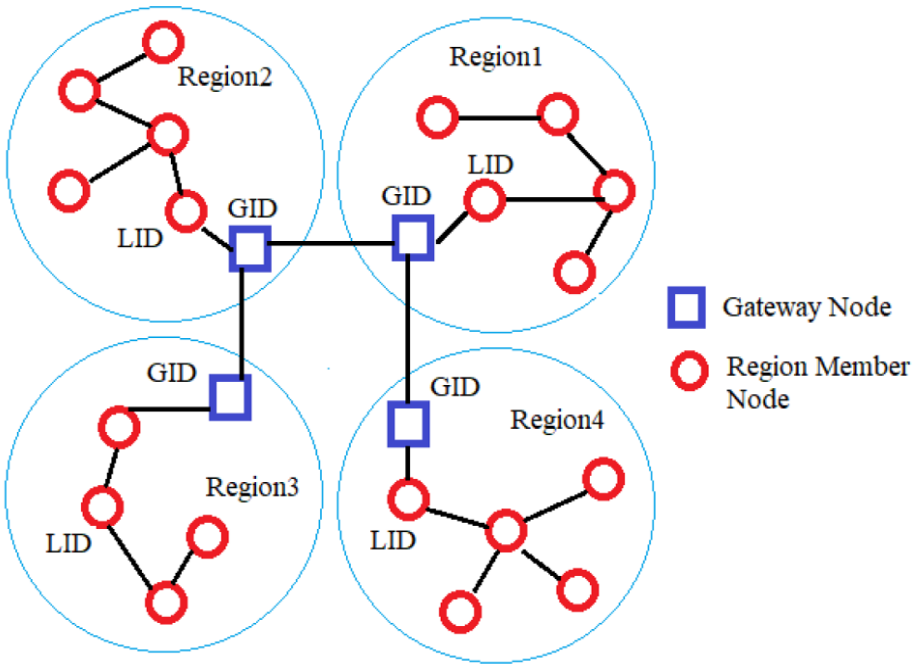

FIGURE 1. The architecture for the region-based intrusion detection

3.1. **Dynamic intrusion detection technique.** The proposed dynamic intrusion detection technique intends to completely automate intrusion detection in a hierarchical and distributed way. The structure of our proposed intrusion detection model consists of two main components that is, Local Intrusion Detection (LID), Gateway Intrusion Detection (GID). In this new hierarchical architecture, every mobile node in MANET network runs a LID locally to perform local data collection and signature based detection and initiates local response, and only some of the nodes, gateway nodes, will run GID, and gateway nodes are organized in multiple layers. GID is shown in Figure 2, containing the Global Detection Agent (GDA), Region Manager Agent (RMA), Global Cooperative Agents (GCA), Global Response Agents (GRA), Region Cooperative Agent (RCA) and Region Response Agent (RRA). In dynamic intrusion detection, a gateway node can optimize energy use by scheduling only a subset of region members who will activate their monitoring sensors agents at one time. Other region members can minimize their energy consumption at the same time. LID is shown in Figure 3, containing the Sensor Agent (SA), Local Detection Agent (LDA) and Local Response Agent (LRA). Alerts are used to

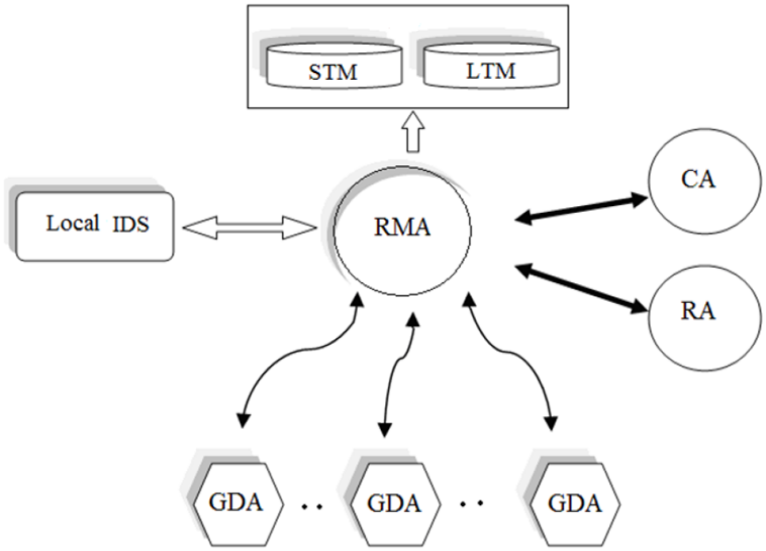

FIGURE 2. Interactions between agents in gateway intrusion detection

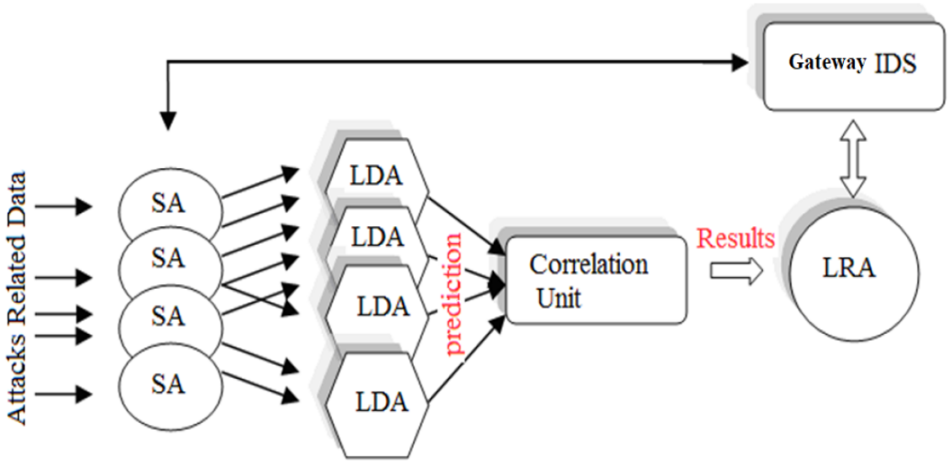

FIGURE 3. Interactions between agents in local intrusion detection

indicate a potential security attack recognized by local intrusion detection agents, while global alarms are finalized decisions made by GID. When a node detects locally an intrusion with strong evidence, depending on some threshold value, the node can initiate a local alarm, by sending an alarm message to the nearest gateway node GID, which in turn triggers local and global response model. This actually starts local response agent and global response agent.

After that, the manager agent stores this alarm in the Long Term Memory (LTM) for further processing. However, if a node detects intrusion with weak or inconclusive evidence and low confident prediction measure, the node initiates local alert to the nearest gateway node GID, which directly starts local and global cooperative intrusion detection procedure, as well as global detection agent GDA, to search for new evidence in long term memory and Short Term Memory (STM), and if any strong evidence discovered, it initiates global and local response model. The global alarm communications among regions are accomplished through manager agents, which share information among different security GID in network's regions. While processes are migrated to detect intrusion or collect special data, mobile agents autonomously migrate to nodes where the information or services are of interest. Communication and execution model is shown in Figure 4. Since

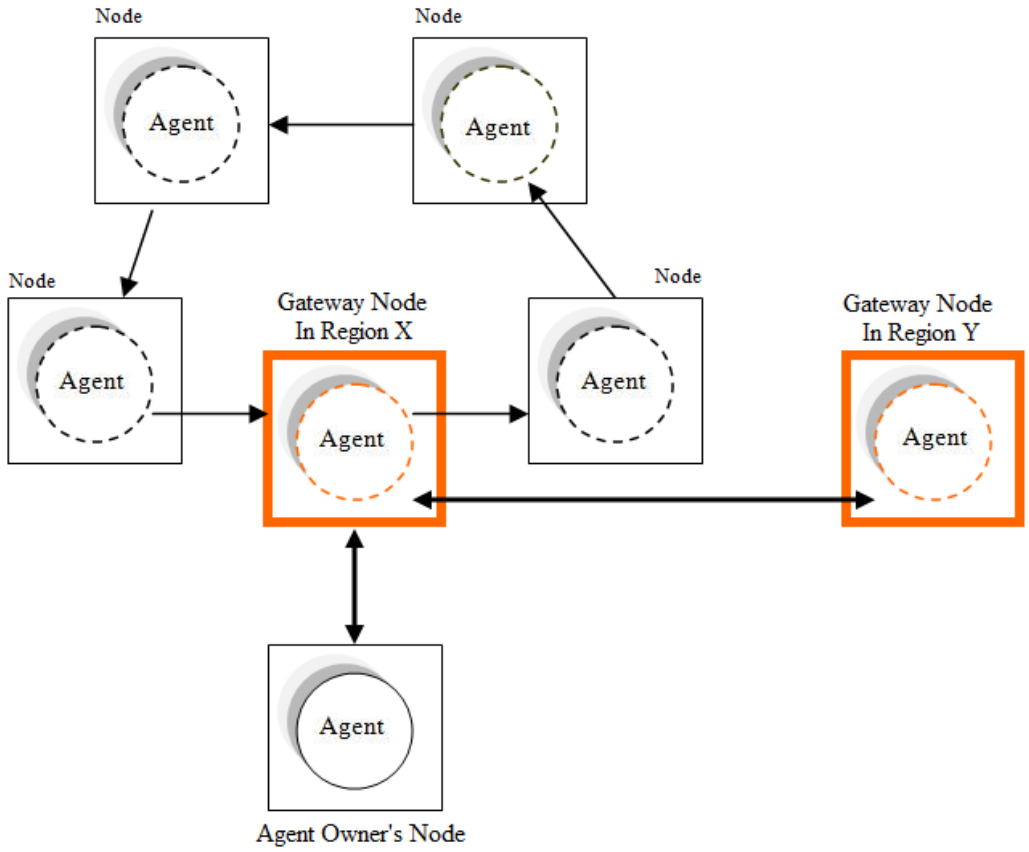

FIGURE 4. Mobile agent communication and execution model

we work in wireless network, the attack can come to the node by one of two ways directly to the node by external attack or by its neighbors (internal attacks). For that, the attacks evidences will be in the same node or with its neighbors. For that reason, the global detection process starts from the gateway node in the central region, then this region will grow by adding its neighbors, and every region adds its neighbors until we get strong evidence with high confidant measures. At the same time, any region that does not have evidence will not participate in the global cooperation decision making process. By using growing region method we can minimize MANET bandwidth and energy consumption for intrusion detection purpose.

3.2. **Agents components in the architecture.** There are several working agents for the proposed architecture. The agents are named as region manager agent, sensor agent, local detection agents, global detection agents, global cooperative agents, region cooperative agents, and response agent. The description of each agent is given below.

Region Manager Agent (RMA): It is in charge of harmonizing all the activities among the models. It assigns the tasks to the other agents and dispatches the mobile agent such as global detection agent, global response agents. Also it performs all the communications between LID agents framework and GID models. As well, it is the heart of the controlling and coordinating with every agent in the region. It maintains the configuration of the agents, records the system status information of each component, and makes the decisions that make other agents work on their duty.

Sensor Agent (SA): Sensor agent in LID collects real-time attack related audit data from more than one source. Attack related data can include user and system data, network routing and data traffic and activity within the radio range of the sensor agent. More than one sensor agent can be utilized by LID.

Local and Global Detection Agents: In these agents the dynamic intrusion detection techniques will be employed. LDA will work on data collecting locally by sensor agent. While GDA will work on local data as well as neighbors' regions data, by dispatching a copy of the agent to those regions.

Cooperative Agents (CA): The functionality of CA is to combine the detection results of different RMA come from all participate regions.

Response Agents: The intrusion response agent is to handle the generated alarms from LDA or RMA.

Short Term Memory (STM): The short term memory is used to store alerts that does not convert to alarm with low conformal prediction measure, in order to be used in future detection process. If GID receives the same alerts from several LID, this alert will be treated special way in GDA.

Long Term Memory (LTM): The long term memory is used to store alarm initiated by RMA and alarm come from other GID from other regions. This memory will be updated periodically. To facilitate communication between agents, we need Agent Communication Language (ACL) [22]. FIPA-ACL is one of the most commonly used languages in MAS [23].

4. **Simulation.** Simulators are the most common tools used for testing the intrusion detection in MANET [3]. Simulators help researchers to study the performance and the reliability of their proposed IDS without using real mobile nodes. In order to evaluate our approach, we simulate a MANET by using Global Mobile information systems Simulation library (GloMoSim). It builds a scalable simulation environment for wireless and wired network systems. Parsec, a C-based simulation language based on parallel discrete-event simulation, is used to design GIoMoSim. We take DSR, one of the popular MANET routing protocols [24], as a case study. In our experiment, we collect trace logs of normal and abnormal data in the GloMoSim simulator. We implement and use the following attacks, Black Hole attack, Selfishness attack and Routing table overflow attack. In our simulation process we consider the following parameters so that they can achieve more practical results, number of nodes used, size of the simulation area, transmission range, traffic send rate and type, number of simulation runs, mobility of the nodes and their speed. True Positive Rate (TPR) and False Positive Rate (FPR) are used to estimate the performance of IDS [19]. TPR measures the number of correctly classified examples relative to the total number of positive examples. FPR measures the number of misclassified positive instances relative to the total number of misclassified instances. We describe the experiments that were conducted to identify the significant network feature that would help detect an attack and identify the intruder. We showed that effective use of dynamic multi-agent can improve the overall detection accuracy. We also illustrated the detection results using different frameworks: dynamic multi-agent intrusion detection model, local intrusion detection systems run on individual node or devices on the MANET network. This model monitors the inbound packets from the device only and will alert admin if suspicious action is detected. Network intrusion detection systems run only on gateway nodes. Table 1 shows the results of the dynamic multi-agent intrusion detection model, local intrusion detection model and network detection all using the same metrics. It shows that the dynamic multi-agent model achieves a higher detection rate than local intrusion detection model. The false positive rate is also decreased. And we note that not less than 20% of the attacks were detected by signature based detection model. Figure 5 shows the Receiver Operating Characteristic (ROC) curves [25] of the performance of network, local and dynamic intrusion detection over three attacks dataset: Black Hole attack, Selfishness attack and Routing table overflow attack. It has been seen that the dynamic multi-agent intrusion detection model achieves a higher detection performance.

TABLE 1. Experimental results on comparison of local and dynamic intrusion detection

	Network detection		Local detection		Dynamic agent detection	
Data set	**TPR**	**FPR**	**TPR**	**FPR**	**TPR**	**FPR**
Black hole attack	0.912	0.062	0.970	0.071	0.99	0.0080
Selfishness attack	0.923	0.07	0.971	0.058	0.98	0.0011
Routing table overflow	0.901	0.081	0.961	0.080	0.99	0.0052

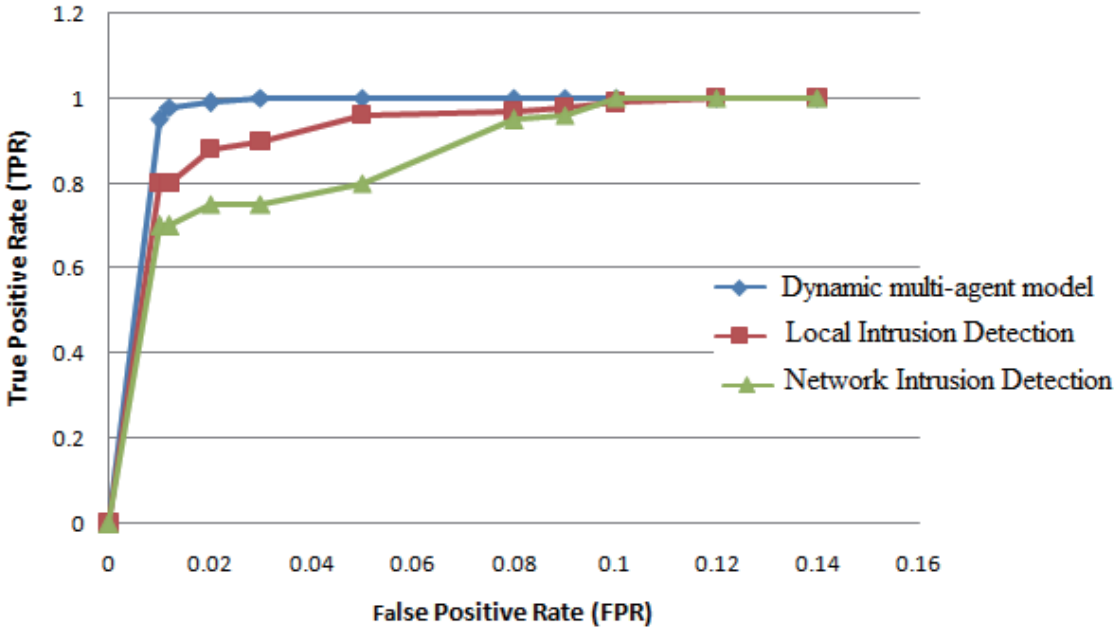

FIGURE 5. ROC curves showing the performance of network detection, local detection and dynamic multi-agent intrusion detection

5. **Conclusion.** We have presented the architecture and operation of dynamic multi-agent intrusion detection technique based on multi agent technology for ad hoc networks, in nonoverlapping region framework. This intrusion detection technique uses static and mobile agents. This fits the distributed nature of MANET. By using multi agent system, we improve the intrusion detection approach to provide new details and information on attack types and sources.

REFERENCES

[1] Y. Zhang and W. Lee, Intrusion detection in wireless ad-hoc networks, *Proc. of MOBICOM 2000*, Boston, pp.275-283, 2000.

[2] R. H. Jhaveri, N. M. Patel, Y. Zhong and A. K. Sangaiah, Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial IoT, *IEEE Access*, vol.6, pp.20085-20103, 2018.

[3] A. F. Farhan, D. Zulkhairi and M. T. Hatim, Mobile agent intrusion detection system for mobile ad hoc networks: A non-overlapping zone approach, *The 4th IEEE/IFIP International Conference on Central Asia on Internet*, Tashkent, pp.1-5, 2008.

[4] H. Otrok, M. Debbabi, C. Assi and P. Bhattacharya, A cooperative approach for analyzing intrusions in mobile ad hoc networks, *The 27th International Conference on Distributed Computing Systems – Workshops (ICDCS Workshops 2007)*, Toronto, ON, Canada, 2007.

[5] N. Marchang, R. Datta and S. K. Das, A novel approach for efficient usage of intrusion detection system in mobile ad hoc networks, *IEEE Trans. Vehicular Technology*, vol.66, no.2, pp.1684-1695, 2017.

[6] S. Rai, R. Boghey and P. R. Yadav, Cluster based energy efficient authentication scheme for secure IDS over MANET, *The 7th International Conference on Communication Systems and Network Technologies (CSNT)*, Nagpur, pp.200-205, 2017.
[7] O. Kachirski and R. Guha, Intrusion detection using mobile agents in wireless ad hoc networks, *Proc. of the IEEE Workshop on Knowledge Media Networking*, pp.153-158, 2002.
[8] F. Abdel-Fattah, K. Farhan, F. Altarawneh and F. Altamimi, Security challenges and attacks in dynamic mobile ad hoc networks (MANETs), *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, Amman, Jordan, pp.28-33, 2019.
[9] Y. Komai, Y. Sasaki, T. Hara and S. Nishio, K nearest neighbor search for location-dependent sensor data in MANETs, *IEEE Access*, vol.3, pp.942-954, 2015.
[10] F. Abdel-Fattah, Z. Md. Dahalin and S. Jusoh, Distributed and cooperative hierarchical intrusion detection on MANETs, *International Journal of Computer Applications*, vol.12, no.5, pp.32-40, 2010.
[11] S. Abbas, M. Faisal, H. Ur Rahman, M. Z. Khan, M. Merabti and A. U. R. Khan, Masquerading attacks detection in mobile ad hoc networks, *IEEE Access*, vol.6, pp.55013-55025, 2018.
[12] F. Abdel-Fattah, Z. Md. Dahalin and S. Jusoh, Dynamic intrusion detection method for mobile ad hoc network using CPDOD algorithm, *International Journal of Computer Applications*, Special Issues on MANETs, no.1, pp.22-29, 2010.
[13] Y.-A. Huang and W. Lee, A cooperative intrusion detection system for ad hoc networks, *Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'03)*, NY, USA, pp.135-147, 2003.
[14] R. Nakeeran, A. Aruldoss and R. Ezumalai, Agent based anomaly intrusion detection system in ad hoc networks, *International Journal of Engineering and Technology*, vol.2, no.1, 2010.
[15] P. Albers, O. Camp, J. M. Percher, B. Jouga and R. Puttini, Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches, *Proc. of the 1st International Workshop on Wireless Information Systems*, pp.1-12, 2002.
[16] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C. Y. Tseng, T. Bowen, K. Levitt and J. Rowe, A general cooperative intrusion detection architecture for manets, *IWIA05: Proc. of the 3rd IEEE International Workshop on Information Assurance*, pp.57-70, 2005.
[17] N. Kominos and C. Douligeris, LIDF: Layered intrusion detection framework for ad-hoc networks, *Ad Hoc Networks*, vol.7, no.1, pp.171-182, 2009.
[18] S. Bose, S. Bharathimurugan and A. Kannan, Multi-layer integrated anomal intrusion detection system for mobile ad hoc networks, *Proc. of the International Conference on Signal Processing, Communications and Networking*, Chennai, 2007.
[19] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe and K. Levitt, A specification-based intrusion detection system for AODV, *Proc. of the 1st ACM Workshop on Security of Ad Hoc And Sensor Networks (SASN'03)*, NY, USA, pp.125-134, 2003.
[20] B. K. Pattanayak and M. Rath, A mobile agent based intrusion detection system architecture for mobile ad hoc networks, *Journal of Computer Science*, vol.10, no.6, pp.970-975, 2014.
[21] T. Anantvalee and J. Wu, A survey on intrusion detection in mobile ad hoc networks, in *Wireless Network Security*, Y. Xiao, X. S. Shen and D.-Z. Du (eds.), Springer, 2006.
[22] Y. Labrou, T. Finin and Y. Peng, Agent communication languages: The current landscape, *IEEE Intelligent Systems*, 1999.
[23] T. Finin, Y. Labrou and J. Mayfield, KQML as an agent communication language, in *Software Agents*, J. Bradshaw (ed.), Software Agents, MIT Press, Cambridge, MA, 1997.
[24] D. B. Johnson, D. A. Maltz and J. Broch, *DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks*, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2001.
[25] A. Slaby, ROC analysis with Matlab, *The 29th International Conference on Information Technology Interfaces*, pp.191-196, 2007.