IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

A Critical Review of Intrusion Detection Systems and Its Applicability in Mobile Ad Hoc Networks

A. Chaudhary[1*], G. Shrimal[2]

[1]Information Technology Department, Manipal University Jaipur, Jaipur, India
[2]Computer Science & Engineering Department, JaganNath University Jaipur, Jaipur, India

[*]*Corresponding Author: alka.chaudhary0207@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 12/Aug/2018, Published: 31/Aug/2018

***Abstract*—** Mobile Ad hoc networks (MANETs) provide autonomous communication between the mobile nodes in the absence of predefined infrastructure. This property of MANETs makes it more vulnerable from conventional networks. Due to this reason, prevention mechanism such as authentication and cryptography techniques alone are not capable to protect it so that intrusion detection system (IDS) employed to facilitate the identification of intrusions in MANETs. This paper examined the detailed analysis on each class of intrusion detection systems that have been proposed in MANETs for preventing the network layer attacks and also focuses the further research areas in MANETs.

***Keywords*—** Mobile Ad hoc Networks (MANETs), Security Issues, Intrusion Detection System (IDS), Detection Architecture and Detection Techniques.

I. INTRODUCTION

The general idea of mobile wireless devices working together was proposed in the mid 1990s. There are some well known groups [1] [2] such as Internet Engineering Task Force (IETF) that is responsible to promote the working of mobile ad hoc networks in terms of developing the routing protocols and also consider the addressing issues. Furthermore, wireless networking offer the two set of wireless services i.e. basic service set (BSS) and independent base service set (IBSS) that are based on IEEE 802.11 standard [3]. Mobile ad hoc networks alleviate the mobile nodes to communicate with each other without the relay on pre defined infrastructure. There is no requirement of any central point during the communication between the mobile nodes.

Due to its dynamic nature, MANETs are worthy for no. of applications such as rescue operations, disaster management, virtual meetings etc. MANETs abide with two properties i.e. multihop and mobility. MANETs features such as wireless links, dynamic topologies and resource constraints make it more prone to security threats [4]. For the security point of view of MANETs, intrusion detection system is an essential part of security for MANETs. It is very effective for detecting the intrusions and usually used to complement for other security mechanism. This paper is organized as follows: Section II, presents the detailed introduction of Intrusion detection system. Section III, introduce the intrusion detection system in MANETs environment and also describes the IDS architectures in MANETs. Section IV, discussed and analyzed the proposed IDSs on MANETs from the literature and finally conclusion and direction for future research is given in section V.

II. INTRUSION DETECTION SYSTEM

Intrusion prevention based techniques such as authentication and encryption are no longer feasible for ad hoc networks so that Intrusion detection system (IDS) is known as the second line of defense for mobile ad hoc networks. When any set of actions make an effort to compromise with the security properties such as confidentiality, integrity, availability of resources and repudiation then these actions are called intrusions and detection of such intrusions are known as intrusion detection system [5]. Intrusion detection system continuously monitors the behavior of the system for detecting any suspicious activity. If it is presented in the system than IDS initiate a proper alarm (e.g. email the Systems Administrator, start an automatic retaliation, etc.)[6].

The functionality of IDS is based on three components i.e. data collection, detection and response. The data collection component collects the data from various sources. It can be host based audit data, network activity traces based data, network packet based or routing table based data etc.

Detection module is responsible to analyze the collected data for detecting the intrusions and then initiate the response by the response module if any suspicious activity detected in the network [7]. Based on the audit data, IDS can be categories as host based and network based where host based IDS emphasized only operating system of a particular host, and network based IDS is responsible to collect the data from network traffic as well as from host also. [8].

Three main detection techniques such as misuse based, anomaly based and specification based, are presented in the literature. The first technique is misuse-based intrusion detection which detects the intrusions on the bases of predefined attack signature. The disadvantage of this technique is that it cannot detect the new attacks but it has low false positive rate so that its generally used by the commercial purpose based IDSs. Second, intrusion detection technique is anomaly-based detection technique. It detects the intrusions on the bases of normal behavior of the system. This technique can able to detect the new or unknown attacks but with high false positive rates. There are various techniques in literature which have been applied for anomaly detection such as statistical approaches, datamining and neural network based approaches. On the other hand, both anomaly-based and misuse-based techniques have their advantages and disadvantages. Third, intrusion detection technique is specification- based detection technique. In this technique, first specified the set of constraints on a particular protocol or program and then detect the intrusions at the run time violation of these specifications. This is alternative technique which has the strength of misuse based and anomaly based detection technique in terms of detecting known and new attacks with low false positive rate. The main problem of this specification based technique is that it takes more time for defining the specification so that it is a time consuming technique. This detection technique has been applied on DHCP (Dynamic Host Configuration Protocol), ARP (Address Resolution Protocol), and MANETs routing protocols such as AODV routing protocol etc. [9] [10]. This technique cannot detect Dos (Denial of Service) attacks because these types of attacks do not directly violate the program specification [11].

III. INTRUSION DETECTION SYSTEMS FOR MANETS ENVIRONMENT

For conventional networks, many IDSs have been proposed but these IDSs cannot be directly applied on mobile ad hoc enviourments due to its different characteristics. MANETs do not have switches, routers or gateways for passing the network traffics like as wired networks. IDSs can easily implement and adjusted with these devices (switches, routers or gateways) in the wired network [12]. In mobile ad hoc networks, mobile nodes do not have any centralized authority for accessing the information to each other. Communication through wireless links makes this network more susceptible to attacks because anyone (both legitimate and malicious users) can join the network and access the information. Some other issues of the MANETs such as cooperativeness, limited resources, mobility makes it different from conventional networks [13]. In the literature, many intrusion detection systems have been proposed which suits the MANETs characteristics that will be discussed in the next sections and also presented the summarization of all reviewed IDSs in Table 1.

IDS Architectures on MANETs

In case of MANETs, suitability of IDS architecture depends on the network infrastructure [14]. Based on infrastructures of mobile ad hoc networks, it can be flat or multilayer according to the applications. In the flat network infrastructure, all nodes of MANETs are considered on the same level (equal), so this type of infrastructure is suitable for such applications i.e. meetings, conferences or virtual class rooms. Moreover, in the multi-layered network infrastructure, all nodes of MANETs are considered on the different level, for this purpose all the network nodes forms the clusters and each cluster has one cluster head. Nodes within the cluster can directly communicate to each other but in case of cross cluster communication it must be accomplished through the cluster heads. This type of infrastructure is suitable for military applications. There is some basic IDSs architecture which designed for MANETs.

1. Stand-alone intrusion detection systems-- In this type of intrusion detection system architecture, IDS run independently on each node. It collects audit data at its own node and behalf on this data detect the intrusions and due to its limitation this type of architecture is not effective. This IDS architecture is suitable for flat network architecture.

2. Distributed and Cooperative Intrusion Detection Systems --In this architecture all nodes take part in intrusion detection. An IDS mobile agents collects the local data and responsible to identify possible intrusions and initiates the local response then the neighboring IDS agents cooperatively responsible for global response. In the same way this architecture is also suitable for flat network infrastructure.

3. Hierarchical Intrusion Detection Systems -- This type of IDS architecture is an extended form of distributed and cooperative IDS architecture in which whole network divides into the clusters. Each cluster has clusterhead which has more responsibility than the other node members in the cluster. Each node in the network has IDS agents. Node members in the cluster are responsible for initiate local response and cluster heads initiates global response. This IDS architecture is suitable for multi-layered network infrastructures.

4. Mobile Agent for Intrusion Detection Systems-- In the mobile agent based IDS, mobile agents is used to perform specific task and then distributes it into each node in the whole networks. It can help to distribute the intrusion detection tasks in the network. Mobile agent based intrusion detection system can be considered in distributed and cooperative based detection method.

IV. PROPOSED IDSs IN MANETs

Since, conventional based IDSs cannot be directly applied on MANETs so that due to this reason many authors have been presented many IDSs for MANETs. In this section, we are going to describe each category of IDSs which has been proposed in Literature.

A. Distributed and Cooperative IDS

Zhang and Lee [15] proposed first distributed and cooperative agent based IDS architecture for mobile ad hoc networks. In this proposed architecture every node participates in intrusion detection and response as shown in Fig. 1. For this aspect each node has an individual IDS agent which is responsible for local and global intrusion detection. For global detection node IDS agent collaborates with neighboring nodes (through secure communication module) whenever available evidence is inconclusive and a border search is needed. When an intrusion is detected an IDS agent triggers a local response (through local response module) or global response (through global response module).

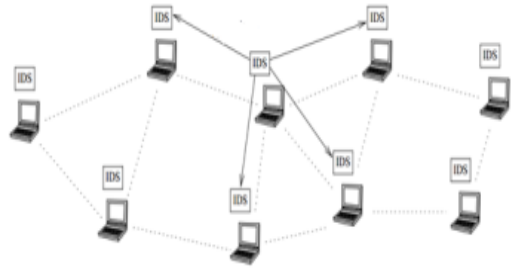

Figure 1. The IDS Architecture for Wireless Ad-Hoc Network [15]

This research chosen only anomaly based detection over misuse- based detection because misuse based detection can detect only known attack and it cannot easily be updated across a wireless ad hoc network. The local data of node is trusted on for statistical anomaly – based detection such as node's movement(distance, direction, velocity) and the change of routing table (PCR: percentage of changed routes, PCH: percentage of changes in sum of hops all the routes). In their subsequent research [16], RIPPER and SVM-Light classification algorithms are evaluated on three routing protocols: AODV, DSR and DSDV using detection rate and false alarm rate metrics. SVM-Light performed better than RIPPER. They stated that the IDS works better with protocols which include some redundancy (such as path redundancy in DSR). Mobility effects are not discussed.

B. IDS Architecture with Stationary Secure Database

Andrew B. Smith [17] proposed a new distributed architecture which consisting of IDS agents and a stationary database (SSD). The IDS agents run on each node in the network and responsible for local detection or global detection (collaborating with other agents in need). Each IDS agent has five parts: local audit trail, local intrusion database (LID), secure communication module, anomaly detection modules (ADMs), and misuse detection modules (MDMs).This proposed architecture has taken advantage of anomaly-based detection using datamining techniques and misused-based detection, but it has a single point failure, the SSD. More important, a stationary node goes to against the nature of MANETs. Implementation and evaluation of proposed architecture are planned for future work.

C. Cross-Feature Analysis based intrusion detection system in MANETs

Yi-an Huang [18] Introduced a new data mining method for automatically constructed an anomaly detection model that are capable of detecting novel or unknown attacks. Data mining method used "cross feature analysis" for capturing inter-feature correlation patterns in normal traffic. With the help of these patterns (normal profiles) classifiers can detect deviation caused by attacks. The basic assumption here for anomaly detection is that normal and abnormal events have different feature vectors that can be separated from each other. They also assumed that all feature values are discrete. It is implemented on Ns-2 simulator under Route logic compromise and Traffic distortion these two categories of attacks. It is the first approach that used feature correlations. They also proposed to investigate how computational cost can be reduced. They also proposed a cluster based IDS architecture in their subsequent research [19] due to resource constraints in MANETs.

D. Zone - Based IDS in MENETs

Bo- sun [20] proposed a non-overlapping zone-based IDS (ZBIDS) architecture. In this architecture, the network divided into non-overlapping zones with the help of geographic partitioning techniques for saving communication bandwidth and improving detection performance. Nodes within the zone are called intrazone node and nodes which work to others zones as a bridge are called gateway nodes. As shown in the fig. 2 the nodes 1, 6, 7 are gateway nodes in zone 5. In the zone, each node is responsible for local detection and sending alerts to other nodes in that particular node. Intrazone nodes are responsible for local aggregation and correlation rather than on behalf of global aggregation and correlation, gateway nodes are responsible to make final decision and send alarms that why only gateway nodes

participated in intrusion detection.
In this paper, authors used only Markov chain anomaly detection in their research and also proposed MIDMEF (MANET Intrusion Detection Message Exchange Format) for exchange information between IDS agents. In their previous work [21] authors focused on mobility using link change rate that reflect different mobility levels. The simulation has been carried out by GlomoSim simulator under the false positive rate, detection rate, and mean time of first alarm (measure for how fast intrusion is detected) based performance matrices. In this paper also proposed MIDMEF (MANET Intrusion Detection Message Exchange Format) for exchanging the information between IDS agents.

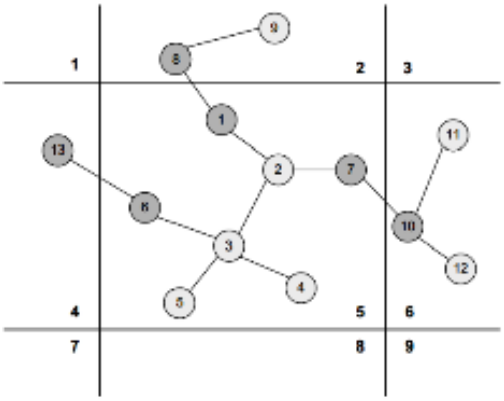

Figure 2. Zone-Based IDS Architecture in MANETs [20]

In future work included plan to investigate other routing attacks scenarios at the routing layer or other layers and further construct security – related features and misuse-based detection approaches.

E. Multiple Sensors based intrusion detection system
In [22] Kachirski and Guha proposed hierarchical and distributed IDS solution which is based on mobile agent technology. This proposed solution provided bandwidth conscious framework, communication cost reduction and improved performance of entire network. This is a significant feature of proposed solution. In this paper, a modular IDS structure is proposed that used three mobile agent classes for performing specific functions. The three mobile agent classes are monitoring, decision-making and action- taking.
The whole network divided into the clusters with the help of given hierarchical and distributed IDS architecture. For choosing cluster head, each node has given vote for a node based on its connectivity. Each cluster have only one sensor agent for packet level monitoring because prevention of resources such as power consumption and battery power of mobile hosts. Cluster head are responsible for detecting on network level data and for decision making. Network intrusion detection performance can change when hop attribute of cluster are changed. In this paper proposed, a bandwidth – efficient IDS but without given validation via simulation or implementation and also detail of the anomaly-based detection technique is not given. Implementation of providing security to mobile agents and intelligent cooperative detection algorithms also included in future work.

F. Specification based intrusion detection system for AODV routing protocol
Chin-Yang Tseng [23] proposed first specification – based intrusion detection system for AODV routing protocol. This paper used distributed network monitor architecture for covering all the nodes in the network. If nodes moving out of the current monitoring area then they are also assumed to move in other network monitors. Actually specification based technique does not detect intrusions or attacks directly. This technique detects intrusions at run time violation of specification. A network monitor used finite state machine as specifications of the operations of AODV such as route discovery process and maintain the forwarding table for each monitored node. In this paper, some of the accepted assumptions are not realistic. This approach can detect known and unknown attacks against routing protocols on the behalf of clearly defined specification. It claimed to detect most of the attacks with minimum overhead in real time. Positions of network monitors in the proposed architecture are not addressed in MANET environment (where frequently topology changes). Other specification – based approaches proposed for AODV is given in [24] [25]. In [24] proposed combination of specification and cryptography approaches. In the literature, there are also few specification based IDSs proposed for OLSR. M. Wang [26] proposed general specification-based intrusion detection for OLSR routing protocol and MRP- based protocols is proposed.

G. Artificial Immune System based IDS for MANETs
Slavisa et al. [27] proposed distributed Intrusion detection system which is based on the Artificial Immune system for MANETs. They are categorized their system into two phases. In the first phase, provided learning to intrusion detection system about the normal behavior of the nodes under the DSR routing protocol. This paper used negative selection and clonal selection algorithms for learning. After completion of learning phase all nodes are entered in the second phase where detection and classification are done. Their system is inspired by the natural immune system (IS) of vertebrates. During implementation, two types of misbehavior implemented in GlomoSim simulator that is non forwarding route requests and non forwarding data packets. This paper, authors defined the primary and secondary (memory based response comes after long time) response. For the future work they planned to propose more misbehavior and traffic patterns.

H. IDS Model integrating Different Techniques
Huang and Lee [28] presented an IDS model which is based

on both specification based and anomaly based detection techniques for the detection of basic events. A basic routing event is defined on causally related routing operation such as receiving/ delivering a packet, modifying a routing parameter. A specification based technique is used to detect those anomalous events that directly violate the specification of AODV routing protocol. They used extended finite state automatas (EFSAs) to represent the specification of AODV routing protocol for specification based technique. For the transition of automata included only these events which are included only local node operations. For the anomaly based technique used a set of detection rule which is generated by using RIPPER classifier. For the evaluation of these techniques they used MobiEmu simulator on some scenarios but in these scenario are not included high degree of mobility during the simulation. The authors presented taxonomy of attacks and also provided a model to detect them. For mobility models, authors can be preferred [29].

I. Finite State Machine based IDS

Ping Yi et al. [30] presented a novel intrusion detection method for mobile ad hoc networks which is based on the finite state machine (FSM). In this architecture used FSM for manually abstracting the correct behaviors of the nodes which are worked according the Dynamic Source Routing (DSR) protocol. With the help of FSM, monitor nodes cooperatively monitor the behavior of every node in the network. They used anomaly based intrusion detection method for detecting real time attacks without any signature and trained data. They evaluated proposed architecture with the help of Ns-2 simulation. On the other hand, the proposed architecture may be time consuming in the case of manually abstracting the behavior of the nodes. Jean-Marie Orset et al. [31] also proposed an extended finite state machine (EFSM) based IDS for ad networks. This paper mentioned the formal specification of the correct behavior of the proactive routing protocol (OLSR) and detection the intrusions at the run time violation of specification. Dina Sadat Jalali et al. [32] provided an new intrusion detection method based on Finite state machine and cache memory based for the ad hoc networks.

J. Distributed Cross-Layer IDS on Ad hoc networks

Yu Liu et al. [33] proposed a distributed cross-layer IDS for MANETs which used rule based datamining anomaly detection technique for detecting the attacks. The proposed IDS can effectively detect attacks and also able to detect attack source within the one-hop perimeter. The architecture of the proposed IDS has four components: data collection module; profile module; detection module and decision module. In their approach they are selected a reduce feature set across the MAC layer and the network Layer for the profile of user normal behaviors. Proposed IDS can only detect the node-based anomaly. So it cannot be detected all types of attack in the network. They evaluated the performance of the proposed architecture using Ns-2 simulation under the four types of attacks (traffic related attacks). This is the first IDS for ad hoc networks which used cross layer detection. S.Bose and A. Kannan [34] presented cross layer based intrusion detection system for detecting the DoS attacks. Rakesh Shrestha et al. [35] also presented a novel cross layer intrusion detection system for detecting malicious nodes and different types of DoS attacks on MANETs. They used cooperative anomaly intrusion detection with data mining techniques for enhancing the detection scheme in proposed architecture. C. J. et al. [36] also provided the integrated cross layer approach for detecting routing attacks on MANETs. For misbehaviors related some other layers such as MAC layer in MANETs, authors can be preferred [37].

K. DEMEM: Distributed Evidence-Driven Message Exchanging Intrusion Detection Model

C.H. Tseng [38] presented a distributed Evidence-Driven Message Exchanging Intrusion Detection Model (DEMEM) in which each node monitored by one- hop neighbor nodes. For exchanging the evidence of intrusions between the nodes authers proposed intrusion (ID) detection massages which known as the term evidence-driven message exchange. With the help of this message one-hop neighbor monitors can exchange the data with 2- hop neighbors. The term Evidence is defined as critical information which is specific to a routing protocol and used this information to validate the correctness of the routing protocol massages such as hop count and node sequence number in AODV. For minimizing the overhead of ID messages, it sent only when only the new evidence happened. In their previous work [39] they proposed specification- based IDS model which is used DEMEM for OLSR routing protocol. They evaluated the DEMEM on the GlomoSim simulator with the mobility under the some attack scenarios such as man-in-middle-attack. When the number of nodes are increased in the network than the DEMEM messages overhead decreased because number of TC and hello messages is more than the ID massages in large networks. It considered that the applicability of DEMEM is more on reactive protocols reason being greater message overhead than the proactive protocols. In their ongoing research include implementing DEMEM in AODV, DSR and TBRPF and a
Reputation based cooperative intrusion response model. [38]

L. Neural network and Watermarking based IDS on MANETs

Aikaterini Mitrokotsa et al. [40] first proposed neural network based intrusion detection system which provided the information visualization for achieving direct response in case of possible intrusions and they used watermarking techniques for the authentication of information visualization. The proposed IDS architecture is composed of multiple local IDS agents that are responsible for detecting the possible attacks on MANETs as shown in figure 10. The

components of local IDS are – Data collector (local audit data and activity logs); Intrusion detection engine; Intrusion response engine. This research paper used eSOM classifier for classifying the normal and abnormal data which based on MAC layer features and after that watermarking technique applied on local eSOM map (normal data) for authentication. Intrusion response engine are responsible for sending local (one hop neighbors of a node) and global alarm (all nodes in a node transmission range). They used combined watermarking techniques (Lattice and Block-Wise method) for authentication of eSOM map. Min-Hua Shao et al. [41] presented a intrusion detection system which is based on the cluster-based cooperative back propagation network approach. Zahra moradi et al. [42] also proposed the neural network based intrusion detection system for MANETs. They can efficiently detect nodes under DoS attack.

M. Grid based Intrusion detection system (IDS)

Pasquale Donadio et al. [43] presented a Grid based intrusion detection system (G-IDS) which are based on the grid computing. It is basically a process or software architecture and applies for intrusion detection mechanisms. It can applicable for both wire and wireless types of networks. It is defined new process which is capable to protect the networks from constantly changing topology. For this reason they used a distributed traffic analyzer that applied the results of real-time feedback sharing between the neighboring nodes of the network. The functioning of proposed architecture is not properly specified in MANETs environments. For the ad hoc network, this system is not specified the attack types and detection techniques.

N. Grammatical Evolution Approach to intrusion detection

S. Sen and John Andrew Clark [44] suggested a grammatical evolution based approach for intrusion detection. They developed programs with the help of this grammatical based approach for some known attacks such as DoS attacks, route disruption attacks. Sevil Sen et al. [45] applied the genetic programming on MANETs and also developed power aware intrusion detection system. This research paper is emphasized for detecting the known attacks. With the help of genetic programming authers are developed the programs separately for each attack such as route request flooding attack and route disruption attack.

This paper showed that one detection program for both attacks can be more energy efficient than detection of these attacks with two separate program. This approach cannot detect the new attacks K. S. Sujatha [46] presented genetic based approach for MANETs. The GA used specification based IDS to detects the attacks on AODV routing protocol. This system analyzes the behavior of the nodes and then detects the attacks.

O. Fuzzy Logic based IDSs for MANETs

Some fuzzy based IDSs also proposed for MANETs. Vydeki Dharmar [47] introduced a fuzzy logic based intrusion detection system for MANETs and proposed standalone architecture based IDS. They applied degree of approximate reasoning to decide upon the degree of maliciousness of particular node and make the decision upon degree of maliciousness of node instead of yes – no decision. For evaluated their approach this paper used Ns-2 network simulator. It can detect some specific attacks. Fuzzy logic based techniques are also applied on cloud computing security [48].

IV. CONCLUSION AND FUTURE WORK

Achievement of trustable security in MANETs is most complex issue due to its dynamic characteristics in these days. Only prevention based techniques such as cryptography and authentication are no longer sufficient for its nature. MANETs works as an open medium for attackers because anyone can join and move the network at any time due to the communication via wireless link. The security mechanism of wired networks cannot be directly applied on MANETs because of its dynamic nature.

In this paper, our main concentration on security of MANETs based on Intrusion detection system. There are many IDSs which have been proposed in literature for MANETs. We have analyzed the working style of some above discussed categories of proposed IDSs and reached decision that still we do not have any promising solution for this dynamic environment. Most of proposed IDSs works on very specific set of attacks and emphasized on specific MANETs issues so that MANETs required more concentration of researchers. It can be a fastest growing area for future research.

ACKNOWLEDGEMENT

We acknowledge A.N.TOOSI (Department of and Information System), University of Melbourne for his useful suggestions.

REFERENCES

[1] IETF Mobile Ad-Hoc Networks Working Group (MANET), IETF web-site www.ietf.org/dyn/wg/charter/manet-charter.html.

[2] IETF Ad-Hoc Networks Autoconfigurations (autoconf) Working Group, IETF website http://datatracker.ietf.org/wg/autoconf/charter/

[3] IEEE Std 802.11-2007, "IEEE standard for information technology-Telecommunication and information exchange between systems- Local and metropolitan area network-Specific requirement, Part 11 Wireless LAN medium access control and physical layer specifications", June 2007.

[4] Chaudhary, Alka, V. N. Tiwari, and Anil Kumar. "A new intrusion detection system based on soft computing techniques using neuro-fuzzy classifier for packet dropping attack in manets." International Journal of Network Security 18, no. 3, 514-522, 2016.

[5] Chaudhary, A., V. N. Tiwari, and A. Kumar. "Analysis of fuzzy logic based intrusion detection systems in mobile ad hoc networks." BVICA M's International Journal of Information Technology 6.1, 2014.

[6] Chaudhary, Alka. "Neuro-fuzzy based intrusion detection systems for network security." Journal of Global Research in Computer Science 5.1, pp. 1-2, 2014.

[7] Lundin E., Jonsson E., "Survey of Intrusion Detection Research", Technical report 02-04, Dept. of Computer Engineering, Chalmers University of Technology, (2002).

[8] Kim J., P. Bentley, "The Artificial Immune Model for Network Intrusion Detection", In 7th European Congress on Intelligent Techniques and Soft Computing (EUFIT'99). Aachen, Germany. September 1999.

[9] Uppuluri P., Sekar R., "Experiences with Specification-based Intrusion Detection. In Proc of the 4th Int Symp on Recent Adv in Intrusion Detect LNCS 2212: 172-189, 2001.

[10] Tseng C-Y, Balasubramayan P. et al., "A Specification-Based Intrusion Detection System for AODV" , In Proc of the ACM Workshop on Secur in Ad Hoc and Sens Netw (SASN), 2003.

[11] Huang Y., Lee W., "Attack Analysis and Detection for Ad Hoc Routing Protocols", In Proc of Recent Adv in Intrusion Detect LNCS 3224:125-145, 2004.

[12] Y. F. Jou, F. Gong, C. Sargor, X. Wu, S. Wu, H. Chang, and F., " Wang, Design and Implementation of a Scalable Intrusion Detection System for the Protection of Networks Infrastructure," Proceedings of DARPA Information Survivability Conference and Exposition, Vol. 2, pp. 69-83, January 2000.

[13] Sevil Şen, John A. Clark "Intrusion detection in mobile ad hoc networks", In Chapter 17, Guide to Wireless Ad Hoc Networks, Springer, 2008.

[14] P. Brutch and C. Ko, "Challenges in Intrusion Detection for Wireless Ad-hoc Networks," Proceedings of 2003 Symposium on Applications and the Internet Workshop, pp. 368-373, January 2003.

[15] Y. Zhang and W. Lee., " Intrusion detection in wireless ad hoc networks" , In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), pages 275-283, 2000.

[16] Y. Zhang, W. Lee, and Y. Huang, "Intrusion detection techniques for mobile wireless networks", In wireless Networks Journal (ACM WINET), September 2003.

[17] A.B. Smith, "An examination of an intrusion detection architecture for wireless ad hoc networks" , In Proceedings of the 5th National Colloquium for Information System Security Education, 2001.

[18] Y. Huang, Wei Fan, Wenke Lee, and Philip S. Yu, "Cross-feature analysis for detection ad-hoc routing anomalies", In Proceedings of the 23rd International Conference on Distributed Computing Systems (ICDCS).

[19] Y. Huang and W. Lee., "A cooperative intrusion detection system for ad hoc net-works", In Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003.

[20] B. Sun, K. Wu, and U.W. Pooch, "Zone-based intrusion detection for mobile ad hoc networks", International Journal of Ad Hoc and Sensor Wireless Networks, 2003.

[21] B. Sun, "Intrusion Detection in Mobile Ad Hoc Networks", PhD thesis, Computer Science, Texas A&M University, 2004.

[22] O. Kachirski and R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks", In Proceedings of the 36th IEEE International Conference on System Sciences, 2003.

[23] C.-Y. Tseng, P. Balasubramayan, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification-based intrusion detection system for AODV", In Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN), 2003.

[24] E. Hansson, J. Gronkvist, K. Persson, and D. Nardquist, "Specification-based intrusion detection combined with cryptography methods for mobile ad hoc networks", Technical report, FOI Swedish Defence Research Agency/Command and Control Systems, 2005.

[25] H.M. Hassan, M. Mahmoud, and S. El-Kassas, " Securing the AODV protocol using specification-based intrusion detection", In Proceedings of the 2nd ACM International Workshop on Quality of Service and Security for Wireless and Mobile Networks, pages 33-35, 2006.

[26] M. Wang, L. Lamont, P. Mason, and M. Gorlatova, "An effective intrusion detection approach for OLSR MANET protocol" ,In Proceedings of the 1st IEEE ICNP Workshop on Secure Network Protocols, pages 55{60, 2005.

[27] S. Sarafijanovic and J. Le Boudec, "An artificial immune system for misbehavior detection in mobile ad-hoc networks with virtual thymus, clustering, danger signal and memory detectors", 2004, pp. 342- 356

[28] Y. Huang and Wenke Lee, " Attack analysis and detection for ad hoc routing protocols" ,In Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pages 125-145, Springer, 2004.

[29] Megat Farez Azril Bin Zuhairi, M., Mohammad Haseeb Zafar, and David Harle. "The impact of mobility models on the performance of mobile Ad Hoc network routing protocol", IETE Technical Review, Vol. 29, No. 5, pp. 414-420, 2012.

[30] Ping Yi, Yiping Zhong, Shiyong Zhang, "A novel intrusion detection method for mobile ad hoc networks in Proceeding EGC'05 Proceedings of the 2005 European conference on Advances in Grid Computing Pages 1183-1192 2005.

[31] J.-M. Orset, B. Alcalde, and A. R. Cavalli, "An EFSM-Based Intrusion Detection System for Ad Hoc Networks", Proc. International Conference on Automated Technology for Verification and Analysis, pp 400–413, 2005.

[32] Dina Sadat Jalali, Alireza Shahrbanoonezhad, " a new intrusion detection method based on fsm and cache memory in ad hoc networks",In Proceedings of IEEE CCIS2011, 2011

[33] L. Yu, L. Yang, and M. Hong, "Short Paper: A Distributed Cross-Layer Intrusion Detection System for Ad Hoc Networks," in Proceedings of the 1st International Conference on Security and

Privacy for Emerging Areas in Communication Networks, Athens, Greece, pp. 418-420, September 2005.

[34] S.Bose and A. Kannan, "Detecting Denial of Service Attacks using Cross Layer based Intrusion Detection System in Wireless Ad Hoc Networks" ,Iin International Conference on Signal Processing, Communications and Networking, ICSCN '08, 2008.

[35] Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi, Seung-Jo Han, "A Novel Cross Layer Intrusion Detection System in MANET ", In 24th IEEE International Conference on Advanced Information Networking and Applications, 2010

[36] C. J. John Felix, A. Das, B.C. Seet, and B.-S. Lee, "CRADS: Integrated Cross Layer Approach for Detecting Routing Attacks in MANETs," in IEEE Wireless Communications and Networking Conference (WCNC), Las Vegas, CA, USA, pp. 1525-1530, March 2008.

[37] .H. Tseng, S.-H. Wang, Wenke Lee, C. Ko, and K. Lewitt, "Demem: Distributed evidence driven message exchange intrusion detection model for MANET", In Proceedings of the 9th International Symposium on Recent Advances in Intrusion Detection (RAID'06), pages 249-271. Springer, 2006.

[38] Sanandaji, A., Jabbehdari, S., Balador, A., & Kanellopoulos, D, "MAC Layer Misbehavior in MANETs", IETE Technical Review, Vo. 30, No. 4, 2013.

[39] C.H. Tseng, T. Song, P. Balasubramanyam, C. Ko, and K. Levitt, "A specification-based intrusion detection model for OLSR",In Proceedings of the 8th International Symposium on Recent Advances in Intrusion Detection (RAID'05), LNCS 3858, pages 330{350. Springer, 2005.

[40] A. Mitrokosta, N. Komninos and C. Douligeris, "Intrusion Detection with Neural Networks and Watermarking Techniques for MANETs", In Proc. IEEE International Conference on Pervasive Services, pp 118-127, July 2007.

[41] Min-Hua Shao, Ji-Bin Lin, Yi-Ping Lee, "Cluster-based Cooperative Back Propagation Network Approach for Intrusion Detection in MANET in IEEE 10th International Conference on Computer an Information Technology (CIT), 2010.

[42] Zahra moradi Mohammad Teshnehlab Amir Masoud Rahmani, " Implementation of Neural Networks for Intrusion Detection in MANET", IN International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT), 2011.

[43] Pasquale Donadio, Antonio Cimmino and Giorgio Ventre "Enhanced Intrusion Detection Systems in Ad Hoc Networks using a Grid Based Agnostic Middleware" , In Proceeding AUPC '08 Proceedings of the 2nd international workshop on Agent-oriented software engineering.challenges for ubiquitous and pervasive computing Pages 15-20, 2008.

[44] S.Sen and John Andrew Clark "A Grammatical Evolution Approach to Intrusion Detection on Mobile Ad hoc Networks", In WiSec '09: Proceedings of the Second ACM Conference on Wireless Network Security March 2009..

[45] S. Sen, J. A. Clark, and J. E. Tapiador, "Power-aware intrusion detection in mobile ad hoc networks", in Ad Hoc Networks, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer Berlin Heidelberg, vol. 28, pp. 224–239, 2010.

[46] Sujatha, K.S., "Design of genetic algorithm based IDS for MANET", In IEEE International Conference on Recent Trends in Information Technology (ICRTIT), 28-33, 19-21 April 2012.

[47] Monita Wahengbam and Ningrinla Marchang, "Intrusion Detection in MANET using Fuzzy Logic", In IEEE 3rd National Conference, pages 189-192 March 2012.

[48] Patidar, V., & Kumbhkar, M., "Analysis of Cloud Computing Security Issues in Software as a Service", International Journal of Scientific Research in Computer Science and Engineering, 2(3), pp. 1-5, 2014.

Authors Profile

Alka Chaudhary received her M.C.A. degree from Institute of Technology and Science (ITS), Mohan Nagar, Ghaziabad in 2010. Currently, she is pursuing M.Tech in Computer Science from Jagannath University Jaipur, Rajasthan. She has published 21 research papers in International Journals and Conferences. Her research interests include Information Security, Mobile Ad Hoc Networks, Neural network, Fuzzy Logic, Intrusion Detection/Prevention, and Network Security.

Gajendra Shrimal is B.E., M.Tech in the field of Computer Science and Engineering. He is currently working as an Assistant Professor in Computer Engineering Department at JaganNath University, Jaipur. His area of interest includes Pattern Recognition & Image Processing. Artificial Intelligence, Randomize Algorithms, and Nature Inspired Computing.

Table 1: Summarization of all reviewed IDSs

IDS	Data Source	IDS Architecture	Detection Technique	Routing Protocol	Addressed attack type	Decision Making	Response Mechanism	Simulator	IDS	Data Source
Distributed and Cooperative IDS [15]	Local data:	Distributed & cooperative	anomaly based detection	AODV, DSR	Abnormal routing updates	Local & collaborative	Active response on attacked system	Ns-2	Distributed and Cooperative IDS [15]	Local data:
Secure stationary database [17]	Host and network audit data	Distributed & cooperative	Anomaly-based and misuse based detection	not specified	not specified	Collaborative	active response on attacked system	–	Secure stationary database [17]	Host and network audit data
IDS using cross-Feature Analysis [18]	Traffic and non – traffic features	Hierarchical, clusters	Anomaly based technique	AODV & DSR	Route logic compromise and Traffic distortion	independent	active response on attacked system	Ns-2	IDS using cross-Feature Analysis [18]	Traffic and non – traffic features
Zone based IDS [20]	changes in routing table	Hierarchical, Zone based	Markov chain anomaly-based detection	DSR	Routing disruption attack	independent	Alarms	GlomoSim	Zone based IDS [20]	changes in routing table
IDS using multiple sensors [22]	User, system and network level data	Hierarchical, distributed & clusters	Anomaly based detection	not specified	Not specified	independent	Active response on attacked system	–	IDS using multiple sensors [22]	User, system and network level data
Specification-Based IDS for AODV [23]	AODV Routing packets	distributed,	Specification detection	AODV	Forged and tunneling attack	Collaborative	Alarm	Ns-2	Specification-Based IDS for AODV [23]	AODV Routing packets
Artificial Immune System based IDS [27]	normal behavior of the nodes	Distributed architecture	anomaly based detection	DSR	Non forwarding route requests	independent	Primary response and secondary response (memory based comes after long time)	GlomoSim	Artificial Immune System based IDS [27]	normal behavior of the nodes
IDS Model integrating Techniques [28]	Local data source of Node	standalone	anomaly and specification based detection	AODV	Flooding	Local	–	MobiEmu	IDS Model integrating Techniques [28]	Local data source of Node
Finite State Machine based IDS [30]	Trace data packets and audit data	Distributed and cooperated	Specification based detection	DSR	Unknown attacks	collaborative	Alarm	Ns-2	Finite State Machine based IDS [30]	Trace data packets and audit data
Distributed Cross-Layer IDS [33]	Audit data (Network activities)	standalone	Anomaly based detection	MAC 802.11 protocol	Traffic related attacks	collaborative	Alert	Ns-2	Distributed Cross-Layer IDS [33]	Audit data (Network activities)
DEMEM [38]	Routing packets of OLSR	Distributed and cooperated IDS	Specification based detection	OLSR	man-in-the-middle attack	collaborative	Active response and recovery on attacked system	GlomoSim	DEMEM [38]	Routing packets of OLSR
Neural network and Watermarking based IDS [40]	local audit and network traffic	Self Organizing Maps	Misused based detection	AODV	Packet dropping attack	independent	Active response on attacked system	Ns-2 eSOM U-matrices	Neural network and Watermarking based IDS [40]	local audit and network traffic
Grid based IDS [43]	Network packets and local traces	Grid computing based architecture	Anomaly based detection	Not specified	Not specified	collaborative	Active response on attacked system	Not specified	Grid based IDS [43]	Network packets and local traces
Grammatical Evolution Approach [44]	Network packet and routing table	Distributed and cooperated architecture	Misuse based detection	AODV	DoS attacks	Local and cooperative	Alarm	Ns-2	Grammatical Evolution Approach [44]	Network packet and routing table
Fuzzy based IDS [47]	Network packet and routing table	standalone	Misused based detection	AODV	Black hole attack, Gray hole attack towards a source and Gray hole	Local	Provide the degree of maliciousness of node	Ns-2	Fuzzy based IDS [47]	Network packet and routing table