Analysis of Fuzzy Logic Based Intrusion Detection Systems in Mobile Ad Hoc Networks

A. Chaudhary[1], **V. N. Tiwari**[2] and **A. Kumar**[3]

Submitted in September, 2013; Accepted in February, 2014

Abstract – Due to the advancement in wireless technologies, many of new paradigms have opened for communications. Among these technologies, mobile ad hoc networks play a prominent role for providing communication in many areas because of its independent nature of predefined infrastructure. But in terms of security, these networks are more vulnerable than the conventional networks because firewall and gateway based security mechanisms cannot be applied on it. That's why intrusion detection systems are used as keystone in these networks. Many number of intrusion detection systems have been discovered to handle the uncertain activity in mobile ad hoc networks. This paper emphasized on proposed fuzzy based intrusion detection systems in mobile ad hoc networks and presented their effectiveness to identify the intrusions. This paper also examines the drawbacks of fuzzy based intrusion detection systems and discussed the future directions in the field of intrusion detection for mobile ad hoc networks.

Index Terms – Detection Methods, Fuzzy Logic, Intrusion detection system (IDS), Intrusion Detection System Architectures, Mobile Ad Hoc Networks (MANETs), Security issues.

1.0 INTRODUCTION

Mobile ad hoc networks (MANETs) do not have any pre-existing infrastructure or administrative point as like conventional networks. In MANETs, mobile nodes can communicate freely to each other without the need of predefined infrastructure. This effectiveness and flexibility makes these types of networks attractive for many applications such as military operations, rescue operations, neighborhood area networks, education applications and virtual conferences. Mobile nodes play the role of host as well as routers and also support the multihop communication between the nodes. By the help of routing protocols, mobile nodes can send the data packets to each other in mobile ad hoc networks. Some characteristics of MANETs such as communication via wireless links, resource constraints (bandwidth and battery power), cooperativeness between the nodes and dynamic topology make it more vulnerable to attacks [1] [2]. Due to Manet's characteristics, Prevention based techniques such as authentication and encryption are not good solution for ad hoc networks to eliminate security threats because prevention based techniques cannot protect against mobile nodes which contain the private keys. So that 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. That's why Intrusion detection system (IDS) is known as the second wall of defense for any survivable network security [3]. There are some groups which works together to enhance the functioning of mobile ad hoc networks (MANETs). IETF constituted the mobile ad hoc networks working group in 1997 [4].The rest of this paper is organized as follows: Section 2 presents the detailed introduction of Intrusion detection system. Section 3 describes the need of fuzzy based IDS on MANETs and Section 4 discusses and analyzes the proposed fuzzy based IDSs in MANETs from the literature. Section 5 discusses the drawbacks of proposed fuzzy based IDS and finally conclusion and direction for future research is outlined in section 6.

2.0 INTRUSION DETECTION SYSTEM

When any set of actions attempt to compromise with the security attributes such as confidentiality, repudiation, availability and integrity of resources then these actions are said to be the intrusions and detection of such intrusions is known as intrusion detection system (IDS) [5]. The basic functionality of IDS depends only on three main modules such as data collection, detection and response modules. The data collection module is responsible for collecting data from various data sources such as system audit data, network traffic data, etc. Detection module is responsible for analysis of collected data. While detecting intrusions if detection module detects any suspicious activity in the network then it initiates response by the response module. There are three main detection techniques presented in the literature such as misuse based, anomaly based and specification based techniques. The first technique, misuse-based detection systems such as IDIOT [6] and STAT [7] detect the intrusions on the behalf of predefined attack signature. The disadvantage of this technique is that it cannot detect new attacks but has low false positive rate so that it is generally used by the commercial purpose based IDSs. Second intrusion detection technique is anomaly-based detection technique e.g. IDES [8]. It detects the intrusion on bases of normal behaviour of the system. Defining the normal behavior of the system is a very challenging task because behavior of system can be changed time to time. This technique can detect the new or unknown attacks but with high false positive rates. The third technique is specification - based intrusion detection

[1,3]Dept. of Computer Science & Engineering, Manipal University, Jaipur (India)-302026
[2]Dept. of Electronic & communication, Manipal University, Jaipur (India)-302026
E-Mail: [1]alka.chaudhary0207@gmail.com,
[2]vivekanand.tiwari@jaipur.manipal.edu and
[3]anil.kumar@jaipur.manipal.edu,

[9]. In this detection method, first specified the set of constraints on a particular protocol or program and then detect the intrusions at run time violation of these specifications. The main problem with this technique is that it takes more time for defining the specification that's why it is a time consuming technique [10]. On the bases of the audit data, Intrusion detection system can be host based and network based. Host based IDS collect the audit data from operating system at a particular host and network based intrusion detection system collects audit data from host as well as trace the network traffic for any type of suspicious activity. Normally there are three basic types of IDS architecture in literature: Stand-alone intrusion detection systems - In this type of intrusion detection system architecture, an IDS run independently on each node in the network; Distributed and Cooperative intrusion detection systems - In this architecture all nodes have IDS agents so that each node can take part in intrusion detection locally and depend on cooperativeness between the nodes it can be made decision globally. This architecture dependent IDS are able to make two types of decision i.e. collaborative and independent. In collaborative decision, all nodes take part actively to make decision but in case of independent decision some particular nodes are responsible for making decision. Hierarchical Intrusion Detection Systems - This type of IDS architecture is an extended form of distributed and cooperative IDS architecture in which whole network is divided into clusters. Each cluster has clusterhead which has more responsibility than the other node members in the cluster [10] [11]. There are many number of IDSs have been proposed in MANETs. We will discuss fuzzy logic based proposed IDSs for MANETs in further sections.

3.0 NEED OF FUZZY BASED INTRUSION DETECTION SYSTEMS

Fuzzy logic is used in intrusion detection since 90's because it is able to deal with uncertainty and complexity which is derived from human reasoning [12]. By the help of fuzzy variables or linguistic terms, intrusion detection features can be viewed easily and decision of normal and abnormal activity in the network are based on its fuzziness nature that can identify the degree of maliciousness of a node instead of yes or no conditions [13] [14]. IF-then-else based fuzzy rules are used to define all situations in the network for identifying the attacks or intrusions. The fuzzy rule based system is known as fuzzy interference system (FIS) that is responsible to take decisions. Many types of fuzzy interference systems are proposed in the literature [15].

4.0 FUZZY BASED INTRUSION DETECTION SYSTEMS IN MANETs

Since, conventional based IDSs cannot be directly applied on MANETs. So due to this reason many authors have presented many IDSs for MANETs. This section is going to describe each category of fuzzy based IDSs which have been proposed in Literature.

1.1 Fuzzy Sets based Agent communication used for tactical MANETs IDS

Domian Walkins [16] proposed stationary intelligent fuzzy agents (SIFA) based IDS for detection of port scanning and distributed DoS attacks in tactical MANETs. Due to the dynamic topology of MANETs it is decided that SIFA resides in each node. For attack recognition, proposed SIFA is dependent on rule based processing system so that reasoning system accomplished with three steps: A knowledge-based, database of derived facts and an interference engine which is used in reasoning logic for processing the knowledge base. This paper used data set for recognition of distributed DoS and port scanning from directly tactical Manet environment. In the large scale Manet's environment, SIFA based IDS could provide overhead.

4. 2 Fuzzy Logic controller based IDS

Sujatha et al. [17] proposed a new fuzzy based response model (FBRM) for the detection of internal attacks in mobile ad hoc network which is depicted in figure 1. In the type of internal attack, they have considered false route request (FRR) attack due to this attack flooding, congestion, DoS attack, exhaustion of resources and exhaustion of bandwidth could happen at nodes in the MANETs. In this scheme Fuzzy logic controller monitors various feature such as route request rate, sequence number, Acknowledgement time and load pattern which can detect FFR attack. The architecture of FBRM is broadly classified into four steps: i) LIDS (local intrusion detection system) log file i.e. for collecting the information based on selected features from each node's local intrusion detection system and also from the neighbors nodes ii) analysis iii) evaluation and iv) response. The overall decision of network state is based on the level of Hacking (LOH) which calculated from sum sequence no., RREQ rate and acknowledge time. LRM (local response module) and GRM (global response module) is responsible for local and global responses.

In global response module, each node sends their response to its neighbor's nodes for global response.

4.3 Biologically Inspired type-2 fuzzy set recognition algorithm based IDS

Andrea and Hooman [18] suggested artificial immune system for detecting misbehaving nodes in Ad-Hoc wireless networks which is based on type-2 Fuzzy set. The purpose of this work is to detect and learn about misbehaviour nodes as well as protect the network without human interference. They assumed that the system is having the different states and any small portion may indicate misbehaviour. This paper used type-2 fuzzy set recognition algorithm for minimizing the uncertainties of some situation in the network where effective network parameter are not well defined for detecting misbehavior nodes, alarm threshold value for selected parameters are not clearly defined, system parameter could be negatively affected by background noise. This paper composed experts knowledge for making the difference between normal and abnormal behavior of selected parameters by the helper T-cells on the bases of person MF (membership function) approach. For reaching the final FOU (Foot print of uncertainty) they used interval type-2 fuzzy map (IT2FM) of each selected parameter

$$\mathrm{IT2FM}\,(fi) \blacksquare \{(x, [\underline{\mu_{fi}}(x), \overline{\mu_{fi}}(x)]), x \in [0, 100]\}$$

Here x percent changes in the parameter f_i is indicated the uncertainty on the behalf of expert knowledge and some indications are used for presenting the changes the parameters such as red region for misbehavior of network parameter f_i, Yellow region for suspicious behavior and white region indicate the normal behavior. Helper T - Cells measure the actual changes of parameter f_i and find the closer region (red, yellow and white) of IT2FM. Once find the final decision then helper T-cells send the signal to Killer T-Cells for particular immune response. Actually, the proposed solution is totally based on the binding process of receptors and antigens. On the other hand, the proposed algorithm could moderate a static artificial immune system because all information of the parameters of the system should be available in advance. So that building the correct type-2 fuzzy map could be inefficient. That' why for future work, they will concentrate on the learning phase of the algorithm.

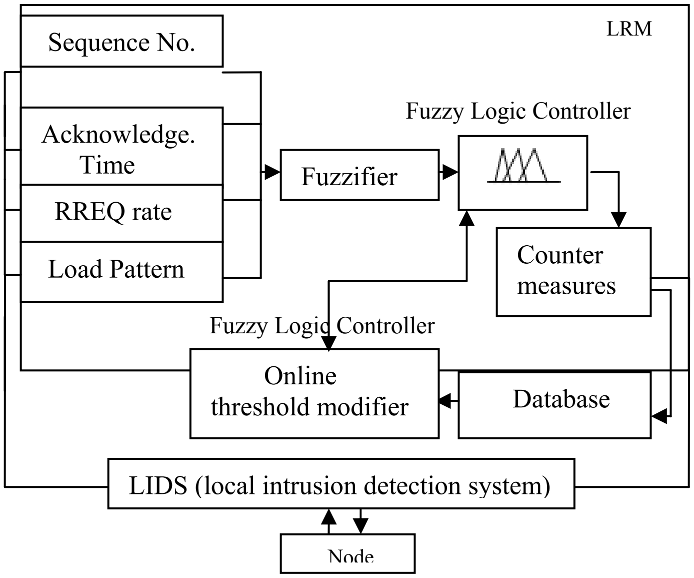

Figure 1: Proposed fuzzy controller based IDS [15]

4.4 Energy based trust solution using Fuzzy logic for MANETs IDS

Vijayan R et al. [19] suggested trust management scheme based on energy utilization using fuzzy logic for detection of selfish nodes in Manets. In the proposed scheme, every node monitors their one hop away neighbours for detection of any kind of malicious behavior with the help of some security components such as supervisor, aggregator, trust calculator and disseminator which is running on each node in the network. In these components, supervisor module is responsible for passively listening to the neighbor's communication with the help of passive acknowledgement (PACK) mechanism to check whether neighbours forwarded the packet or not. Aggregator module calculates the number of packets dropped and based on this each node trust level is determined. Third module trust calculator is calculated with the trust level by using percentage of packet dropped from the previous module. In this module fuzzy logic is used to calculate the trust level where percentage of packet dropped treated as fuzzy input variable. However, fuzzy trust calculator is based on direct trust agent, indirect trust agent and aggregator functionality where aggregator evaluated the total trust values. For total energy measurement at node to another node can be determined as follows:

$$E_{y/x} = P_{n>0}\,(P_{x=y}\,E_{Tack} + P_{x \neq y}\,E_{Rack}) + P_{m>0}\,(P_{x=y}\,E_{Tpck} + P_{x \neq y}\,E_{Rpck})$$

Where $E_{y/x}$ energy spent at node Y to node X, E_{Tack} and E_{Tpck} energy spent at transmit one acknowledgment and one data packet or E_{Tpck} and E_{Rack} energy spent at received one acknowledgment and one data packet. This defined equation and disseminator module is used to get the trust value in the case of mobility of the nodes in the network. They used network simulator NS-2 for carried out the simulation of proposed scheme in the network. At the time of calculation of trust level such factors i.e. link broken, battery exhaustion and replay packet generated are not considered so that it could degrade the accuracy level of proposed scheme.

4.5 Fuzzy Logic based IDS for MANETs

Kulbhushan and Jagpreet [20] proposed a fuzzy logic based IDS which can detect black hole attack on MANETs which is presented in figure 2. They formed the rule for detecting attack based on Mamdani fuzzy model and for drawing the membership function, input parameters such as forward packet ratio and average destination sequence number selected in each time slot. The output of derived rule is dependent on the fidelity level of each node which value is between 0 to 10 and threshold fidelity level chosen 5.5 for analyzing the level of node. If calculated fidelity level of node is less than or equal to fidelity threshold value then node is blackhole otherwise node is not blackhole. Ultimately fidelity level shows the level of node.

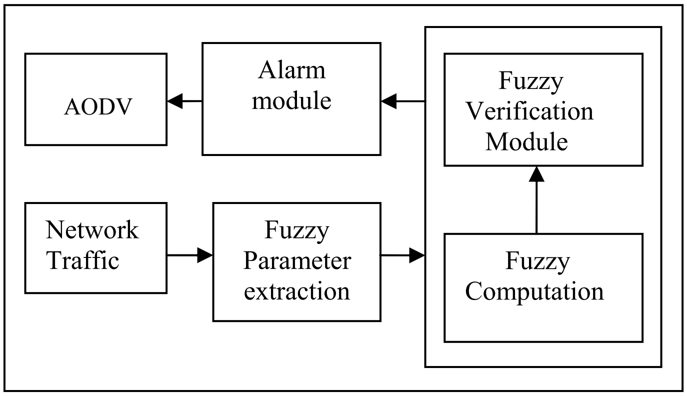

Figure 2: Proposed fuzzy based IDS [18]

This scheme is helpful for detecting blackhole attack but cannot detect new attack. In literature, there are other approaches also available for detecting blackhole attack using fuzzy logic such as M. Wahengbam et al. [21] suggested a fuzzy based IDS for MANETs which is capable to detect packet dropping attack such as Black hole and Gray hole attack. They considered that each node is having IDS and detect malicious activity locally for this purpose and assumed some threshold value for each node. In this proposed approach, each node maintains its packet list with the feature: sequence no., source node, destination node, packet type and expire time. During analysis, they calculated some indications on the bases of degree of symptoms, frequency of occurrence of symptoms and confirmed the presence of attack. Using NS-2 simulator, they have tested their scheme in two ways: when fuzzy logic is used for detection process and when fuzzy logic is not used. On the bases of analysis result, it proved that the fuzzy logic is more capable to find proposed attack accurately. This scheme chosen the threshold value for each node is very confusing job.

4.6 Trust and fuzzy logic based security framework for MANETs

Manoj V. et al. [22] presented a scheme based on certification authority (CA) and fuzzy logic for MANETs. Some central node is authorized by service provider for assigning the keys to source node which is going to request in the network called certification authority nodes and with the help of trust agent, direct and recommended trust values are obtained periodically. Direct and recommended trust values are calculated from direct observation of one hop away neighbors with the help of algorithms. A proposed fuzzy logic based analyzer used to calculate the trust value of a requested node (which is ready to data exchange between source and destination in the network) based on the computed fuzzy table. If requested node is trusted then it would get the certification otherwise not. Fuzzy logic based analyzer has total control on CA nodes. They have tested their approach on Qualnet simulator 5.0 with 6 and 12 no. of nodes. In this approach any one trusted node could be compromised with malicious node due to the communication via wireless link in MANETs.

4.7 Fuzzy based hybrid intrusion detection system for mobile ad hoc networks:

Vydeki et al. [23] used Fuzzy interference system (sugeno type-2) for detection of Black hole attack in Manet and proposed architecture is depicted in

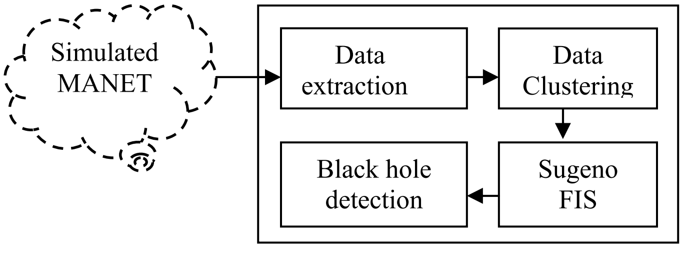

Figure 3: FIS based IDS [21]

They advised that selection of clustering algorithm in the process of FIS based IDSs play an important role so that it compared two well known clustering approaches such as subtractive and Fuzzy c-mean clustering. This proved that the detection rate based subtractive clustering (97%) is more efficient than the fuzzy c-means clustering (91%). This proposed approach only detects the black hole attack.

4.8 Forensic Analysis based on fuzzy Approach for IDS in MANET

Sarah and Nirkhi [24] introduced fuzzy logic based approach for forensic analysis to detect the distributed denial of service attacks (DDoS) in Manets. They suggested use of forensic analysis for intrusion detection because it is able to gather digital evidences from any system which has been compromised. It can reconstruct the compromised system and identify the location of attacker. This paper uses fuzzy Logic approach to forensic analysis based on dynamic source routing (DSR) protocol. Three steps are followed to get the result as a forensic report: first capture the log files then analyzing log files using fuzzy logic and at last presenting the conclusion in terms of forensic report. However, in this paper no simulation and experimental results based on forensic analysis are given.

4.9 Mamdani and Sugeno Fuzzy Inference Systems based IDSs in MANETs:

Alka C. et al. [25] [26] [27] proposed mamdani and sugeno fuzzy inference systems based IDSs for packet dropping attack (PDA) and sleep deprivation attack (SDA) in MANETs. The simulation results are proved that the proposed systems are able to detect the PDA and SDA attacks very efficiently in MANETs.

5.0 DRAWBACKS IN PREVIOUS PROPOSED FUZZY BASED INTRUSION DETECTION SYSTEMS

The proposed fuzzy based IDSs for detection of intrusions in MANETs are not able to cope up all type of attacks. One of few proposed IDSs can cope attacks [18] but it is also having some limitations. We have analyzed that all proposed fuzzy based IDSs are considered very limited features or attributes for data collection which is specific for a particular attack. So that these IDSs are only detect the particular attack in MANETs. In IDS Architecture point of view, due to the complex properties of mobile ad hoc networks are required distributed and cooperated architecture but some of proposed IDSs are concentrated only distributed architecture that's why these IDSs only detect the attacks locally. In case of local detection, each node are only responsible for raise alarm when it detects intrusion locally or not shared it to other nodes in the network for global detection. In terms of detection techniques, as per Table 1 presented that the most of proposed fuzzy based intrusion detection systems use misuse detection techniques and very few fuzzy based IDSs use anomaly and specification based detection techniques. However misused detection technique is responsible for detecting limited attacks i.e. membership function in fuzzy based approaches are defined for only specific attack so that these fuzzy based detection approaches cannot be detect new malicious activity or attacks that's why selection of detection techniques should be anomaly based or hybrid. Table 1 summarizes all fuzzy based IDSs in MANETs.

6.0 CONCLUSION AND FUTURE SCOPE

In this paper, we have analyzed fuzzy based intrusion detection systems which have been proposed in literature for Manets. We have analyzed the working style of proposed fuzzy based IDSs and reached on decision that still we do not have any promising solution for this dynamic environment because most of Proposed fuzzy based IDSs emphasized on very limited features for data collection towards detection of very specific range of attacks. Hence, MANETs are required for more concentration of researchers. It can be a fastest growing area for future research in terms of detection techniques, response mechanism and selection of node features for data collection. In future, we are concentrating to develop a new intrusion detection system that can be used to classify the normal and malicious activities in the network.

REFERENCES

[1]. Y. Li and J. Wei., “Guidelines on selecting intrusion detection methods in MANET”, In Proceedings of the Information Systems Educators Conference, 2004.

[2]. A. Hasti, “Study of Impact of Mobile Ad – Hoc Networking and its Future Applications”, BIJIT – 2012; January - June, 2012; Vol. 4 No. 1; ISSN 0973 – 5658.

[3]. 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.

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

[5]. R. Heady, G. Luger, A. Maccabe, and M. Servilla, “The architecture of a network level intrusion detection system” Technical report, Computer Science Department, University of New Mexico, August 1990.

[6]. S. Kumar and E. H. Spafford, “A software architecture to support misuse intrusion detection” In Proceedings of the 18th national Information Security Conference, pages 194- 204, 1995.

[7]. K. Ilgun, R. A. Kemmerer, and P.A. Porras, “State transition Analysis: A rule- based intrusion detection approach”, IEEE Transactions on software Engineering, Vol. 21 No. 3:181-199, March 1995.

[8]. T.Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P.Neumann, H. Javitz, A. Valdes, and T.Garvey, “A real- time intrusion detection expert system (IDES) – final technical report”, Technical report, Computer Science Laboratory, SRI International, Menlo Park, Clifornia, February, 1992.

[9]. Uppuluri P, Sekar R, “Experiences with Specification-based Intrusion Detection”, In Proc of the 4th Int Symp on Recent Adv in Intrusion Detection , pp. 172-189. 2001.

[10]. S. Sen, J.A. Clark - Guide to Wireless Ad Hoc Networks; In: Chapter 17-Intrusion Detection in Mobile Ad Hoc Networks-Springer, 2008.

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

[12]. B. Shanmugam and N. B. Idris, “Anomaly Intrusion Detection based on Fuzzy Logic and Data Mining”, In Proceedings of the Postgraduate Annual Research Seminar, Malaysia 2006.

[13]. M. Wahengbam and N. Marchang, “Intrusion detection in manet using fuzzy logic”, 3rd IEEE National Conference on Emerging Trends and Applications in Computer Science (NCETACS), ISBN: 978-1-4577-0749-0, pp. 189 – 192, Shillong, 30-31 March 2012.

[14]. Verma, A. K., R. Anil, and Om Prakash Jain. "Fuzzy Logic Based Revised Defect Rating for Software Lifecycle Performance Prediction Using GMR."Bharati Vidyapeeth’s Institute of Computer Applications and Management, 2009.

[15]. J. S. R. Jang, C. T. Sun and E. Mizutani – Neuro-Fuzzy and Soft Computing - A computational Approach to Learning and Machine Intelligence; First Edition; Prentice Hall of India, 1997.

[16]. Watkins, Damian. "Tactical manet attack detection based on fuzzy sets using agent communication." In 24th Army Science Conference, Orlando, FL, 2005.

[17]. S. Sujatha, P. Vivekanandan, A. Kannan, “Fuzzy logic controller based intrusion handling system for mobile ad hoc networks”, Asian Journal of Information Technology, ISSN: 1682- 3915, pp.175-182, 2008.

[18]. A. Visconti, H. Tahayori, “ A Biologically – Inspired type-2 fuzzy set based algorithm for detecting misbehaving nodes in ad hoc networks” , International Journal for Infonomics, Vol.3, No.2, pp. 270-277, June 2010.

[19]. R. Vijayan, V. Mareeswari and K. Ramakrishna, “Energy based trust solution for detecting selfish nodes in manet using fuzzy logic”, International Journal of research and reviews in computer science , Vo. 2, No. 3, pp. 647-652, June 2011.

[20]. Kulbhushan and Jagpreet Singh, “Fuzzy logic based intrusion detection system against blackhole attack AODV in manet”, IJCA Special issue on “Network Security and Cryptography” Vol. NSC, No. 2 pp. 28-35, December, 2011.

[21]. M. Wahengbam and N. Marchang, “Intrusion detection in manet using fuzzy logic”, 3rd IEEE National Conference on Emerging Trends and Applications in Computer Science (NCETACS), ISBN: 978-1-4577-0749-0, pp. 189 – 192, Shillong, 30-31 March 2012.

[22]. V. Manoj, M. Aaqib, N. Raghavendiran and R. Vijayan “A Novel security framework using trust and fuzzy logic in manet” , International Journal of Distributed and

Parallel Systems , Vol. 3, No. 1, pp. 285-298, January,2012

[23]. D. Vydeki and R.S. Bhuvaneswaran, “Effect of clustering in designing a fuzzy based hybrid intrusion detection system for mobile ad hoc networks”, Journal of Computer Science, Vol. 9, No. 4, pp. 521-525, ISSN: 1549 - 3636, 2013.

[24]. S. Ahmed & S.M. Nirkhi, “A Fuzzy approach for forensic analysis of DDoS attack in manet” International Conference on Computer Science and Information Technology, ISBN: 978-93-82208-70-9, Hyderabad, 10th March 2013.

[25]. Chaudhary, A., Kumar, A., & Tiwari, V. N. (2014, February), “ A reliable solution against Packet dropping attack due to malicious nodes using fuzzy Logic in MANETs”, In Optimization, Reliability, and Information Technology (ICROIT), 2014 International Conference on (pp. 178-181), IEEE.

[26]. Chaudhary, A., Tiwari, V. N., & Kumar, A. (2014, February), “Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc network”, In Advance Computing Conference (IACC), 2014 IEEE International (pp. 256-261), IEEE.

[27]. Chaudhary, A., Tiwari, V. N., & Kumar, A. (2014, February), “Design an Anomaly Based Novel Approach for Detection of Sleep Deprivation Attack in Mobile Ad hoc networks Using Soft Computing”, Proceedings of 3rd International Conference on Recent Trends in Engineering & Technology (ICRTET’2014), Elsevier.

IDS	**Data Source**	**IDS Architectures**	**Detection Techniques**	**Routing Protocol**	**Addressed attack type**	**Decision Making**	**Response Mechanism**	**Simulator & Toolbox**
IDS using Fuzzy Sets based Agent communication [16]	Collect packet data from data stream	Distributed & cooperative	Misuse based detection	not specified	Distributed denial of service attacks and port scanning attacks	Independent & collaborative	Alarm	SIFA Application
Fuzzy Logic Controller based IDS [17]	LIDS audit log file and neighbors related data	Distributed & cooperative	Misuse based detection	AODV	False route request attack	collaborative	Fuzzy based response model on attacked system	NS-2 and fuzzy logic controller toolbox of MATLAB 6.1
Artificial Immune System based on Type-2 Fuzzy Sets for Manets IDS [18]	Collect sample data of various network parameters	Distributed & cooperative	Partial-Anomaly based detection	not specified	Misbehaving Nodes	collaborative	Active immune based response on attacked system	No detail
Energy based trust solution using fuzzy logic for IDS[19]	network packet level data	Distributed	Anomaly based Detection	DSR	Selfish nodes	Independent	No detail	NS-2

IDS	Data Source	IDS Architectures	Detection Techniques	Routing Protocol	Addressed attack type	Decision Making	Response Mechanism	Simulator & Toolbox
Fuzzy logic based IDS [20]	Network traffic related feature	Distributed	Misuse based detection	AODV	Blackhole Attack	Independent	Alarm	NS-2
IDS using Fuzzy Logic[21]	Packet related feature	Distributed	Misuse based detection	AODV	Blackhole Attack, Gray hole Attack	Independent	Active response	NS-2
Trust and fuzzy logic based IDS[22]	Network packet data	Distributed & cooperative	Cryptographic algorithms and trust based	AODV	Malicious node	collaborative	alarm	Qualnet 5.0
Fuzzy inference system based IDS[23]	Data packets and control packet based features	Distributed	Specification and anomaly based detection	AODV	Blackhole attack	Independent	Active response based on FIS system output	NS-2 and MATLAB Function 'genfis'
IDS using Forensic analysis based on fuzzy logic approach[24]	Data packets and routing packets	Distributed	Misuse based detection	DSR	Distributed denial of service attacks	Independent	not specified	_
Mamdani and Sugeno based IDSs [25][26][27]	Packet based and mobility based data	Distributed Architecture	Misuse based And anomaly based	AODV	Packet dropping attack and sleep deprivation attack	Independent	alarm	Qualnet Simulator 6.1

Table 1: Summarization of All Reviewed Fuzzy Based IDSs