FIDSM: Fuzzy based Intrusion Detection Systems in Mobile Ad Hoc Networks

Priyanka Dahiya
CSE, Manipal University jaipur, India

Alka Chaudhary
CSE, Manipal University jaipur, India

ABSTRACT

Security of mobile ad hoc networks is more challenging task due to its complex properties. In mobile ad hoc networks, intrusion detection system is known as the second line of defense because prevention based techniques are not a good solution for ad hoc networks due to its complex characteristics. For the security point of view, many intrusion detection systems have been proposed to mobile ad hoc networks in literature. This paper analyzed the proposed fuzzy logic based intrusion detection systems in mobile ad hoc networks.

Keywords

Mobile ad hoc networks (MANETs), MANETs security issues, Intrusion detection system (IDS) and Fuzzy logic

1. INTRODUCTION

Mobile ad hoc networks are more flexible for communication between mobile nodes because there is no need of any pre-existing infrastructure or administrative point. MANETs facilitate mobile nodes can freely communicate 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, neighbourhood area networks, education applications and virtual conferences.

During the communication under routing protocols, mobile nodes cooperate to each other for sending data packets from source to destination that's why MANETs support the multihop communication between the nodes or two nodes can communicate or send data packets directly to each other when they come within the radio range to each other's [1].

An Intrusion detection system dynamically monitors a system and user actions in the system to detect the intrusions [2]. The basic functionality of IDS depends only on three main components such as data collection, detection and response. The data collection component is responsible for collecting the data from various data sources such as system audit data, network traffic data, etc. In detection module is responsible to analysis of collected data for detecting the intrusions and if detection module are detected any suspicious activity in the network then initiate the response by the response module.

There are mainly three detection techniques such as misuse based, Anomaly based and specification based techniques presented in the literature [3].Misuse-based detection systems detect the intrusions on the behalf of predefined attack signature. Second intrusion detection technique is anomaly-based detection technique. It detects the intrusion on bases of normal behavior of the system. The third technique is specification - based intrusion detection. In this detection method, 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 paper emphasized on proposed fuzzy logic based intrusion detection system in mobile ad hoc networks. Fuzzy logic is used in intrusion detection before since 90's because it is able to deal with uncertainty and complexity which is derived from human reasoning [4]. 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 be identified the degree of maliciousness of a node instead of yes or no conditions [5].

In the rest of paper are organized as follows: in section 2 analyze the proposed fuzzy logic based intrusion detection system and section 3 presents the conclusion in terms of results.

2. FUZZY LOGIC BASED INTRUSION DETECTION SYSTEMS IN MANETS

This section is going to present some popular fuzzy logic based intrusion detection systems for mobile ad hoc networks which have been proposed in literature.

2.1 Intrusion Detection System Based on Fuzzy Logic Controller

Sujatha et al. [6] proposed a fuzzy based response model (FBRM) to detect the internal attacks in MANETs that is depicted in fig. 1. This paper considered false route request (FRR) attack that also can be caused many other attacks in network such as flooding, congestion, DoS attack, exhaustion of resources and exhaustion of bandwidth.

For the detection of false route request (FRR) attack, fuzzy logic controller monitors the various features such as route request rate, Acknowledgement time, load pattern and sequence number in the network.

The FBRM architecture mainly have four modules: LIDS log file, Analysis, Evaluation and response. The complete decision regarding network state is based on the level of Hacking (LOH) which calculated from sum sequence no, RREQ rate and acknowledge time.

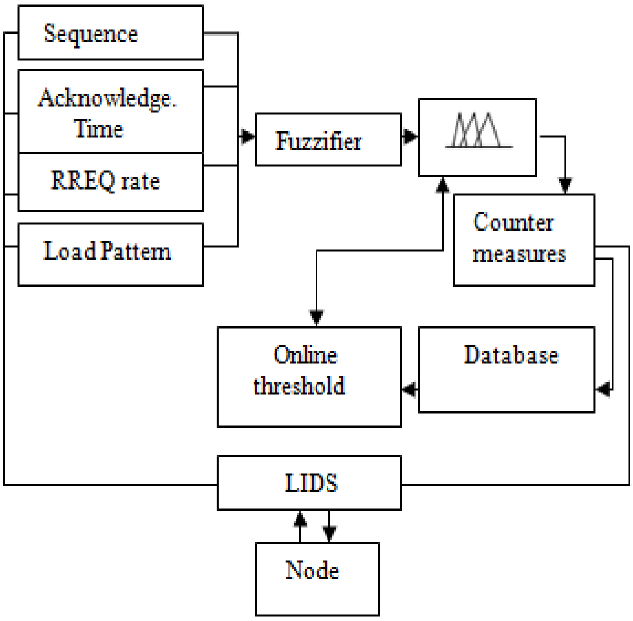

Fig. 1: Fuzzy controller based IDS [6]

2.2 Forensic Analysis based on Fuzzy Approach for IDS in MANET

Sarah and Nirkhi [7] presented forensic analysis based on fuzzy logic for detecting the distributed denial of service attacks (DDoS) in mobile ad hoc networks. This paper suggested the forensic analysis for the detection of intrusions or attacks from the networks because forensic analysis can be gathered digital evidence from any system that has been compromised.

Forensic analysis can be identified the location of attacker and also reconstruct the compromised system. During the forensic analysis, three steps are follows to reach any conclusion as a forensic report i.e. first capture the log files, analyze log files using fuzzy logic and lastly presents the conclusion in terms of forensic report.

2.3. Combinatorial Approach for Design of fuzzy based IDS

Vydeki and Bhuvaneswaran [8] proposed a fuzzy logic based intrusion detection system to detect the black hole attack in MANETs. This paper used combination of specification and anomaly based detection methods. This paper used fuzzy inference system for making the fuzzy rules to take the decision. There are some parameters for checking the behaviour of node is malicious or not.

such as route request forwarding rate, no. of route replies sent and number of packets dropped by each node. in this paper also describe the advantage and disadvantage of mamdani and sugeno fuzzy inference system. For the anomaly detection they have set threshold value to detect the malicious node i.e. black hole node. The functionality of fuzzy logic is given in the fig. 2.

The proposed approach performance in this paper presented the high detection rate and low false positive rate against black hole attack under different level of traffic rate.

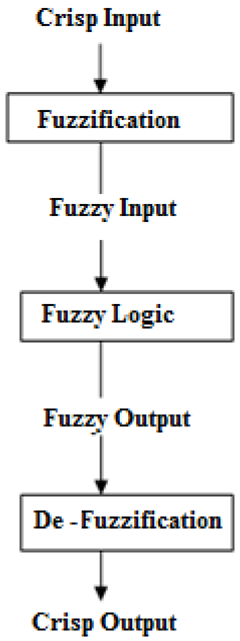

Fig. 2: Fuzzy logic functionality [8]

2.4 Fuzzy based Integrated Security Model for MANETs

M. B. Mukesh Krishnan and P. Sheik Abdul Khader [9] proposed an integrated security model for MANETs. As an integrated point of view, this paper integrates the authentication key and intrusion detection system through fuzzy approach together for providing the dual defense of this dynamic enviourments i.e. MANETs.

They have concentrated various attacks during their simulation and also compared with simulation of various authentication key and intrusion detection models. The results showed that the integrated security model presented better performance against without integration of authentication key and intrusion detection system through fuzzy logic based approaches.

2.5 Sugeno and Mamdani based Intrusion Detection Systems for MANETs

Alka et al. [10] [11] presented mamdani and sugeno fuzzy inference systems based intrusion detection systems (IDSs) for packet dropping attack. The simulation results show that the proposed IDSs are able to identify the packet dropping attack.

2.6 Mamdani Fuzzy Inference based IDS for MANETs

Alka et al. [12] also proposed the mamdani fuzzy inference system based IDS for sleep deprivation attack. The proposed approach identified the sleep deprivation attack in distributed manner from each node. This paper presented the fuzzy rule base for detecting the sleep deprivation attack in network. simulation results show that the proposed scheme are able to detect sleep deprivation attack very efficiently.

3. CONCLUSION

In this paper, we have analyzed fuzzy logic based intrusion detection systems for mobile ad hoc networks. As a result, there are few IDS are proposed in literature which is based on fuzzy logic. These proposed IDSs have emphasized only few features for data collection and few specific attacks in MANETs. For the future aspect, there is need for new IDS which can cover all features for data collection towards all attacks.

4. 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] Bo Sun and Lawrence Osborne: Intrusion detection techniques in mobile ad hoc and wireless sensor network. In: IEEE Wireless Communications,1536-1284, 2007.

[3] R. Heady, G. Luger, A. Maccabe, and M. Servilla, "The architecture of a network level intrusion detection system" Technical National Conference on Emerging Trends and Applications in Computer report, Computer Science Department, University of New Mexico, August 1990.

[4] 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.

[5] M. Wahengbam and N. Marchang, "Intrusion detection in manet using fuzzy logic", 3rd IEEE Science (NCETACS), ISBN: 978-1-4577-0749-0, pp. 189 – 192, Shillong, 30-31 March 2012.

[6] 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.

[7] 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.

[8] Vydeki Dharmar and R.S. Bhuvaneswaran, "A combinatorial approach for design of fuzzy based intrusion detection system", proc. of international conference on computer applications (ICCA) 2012.

[9] M. B. Mukesh Krishnan, P. Sheik Abdul Khader, "Fuzzy Based Integrated Security Model for Mobile Ad Hoc Network", Global Trends in Computing and Communication Systems Communications in Computer and Information Science Volume 269, 2012, pp 467-472.

[10] 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.

[11] 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.

[12] 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.