Intrusion Detection System in Manets

M.Durairaj, S.Dilipkumar

Abstract: One of the most challenging issue nowadays is providing security on MANET architecture. The key issue in MANET is the design of intrusion detection system, that is able to detect attacks in a rapid manner .Traditional methods like genetic algorithms, fuzzy logic, game theory techniques are helpful in designing of IDs. However, these techniques have a limitation on the effects of prevention techniques in general and they are designed for a set of known attacks. These techniques are also tends to increase the false positive ratio, detection rate is low and values of ROC characteristics due to training of feature set of attack patterns . The techniques also failed to detect any new type of attacks by any existing methods. This paper focuses on designing of intrusion detection system based on hybrid approach that effectively able to detect *any type of attacks using Evolutionary algorithm techniques.*

Keywords: Intrusion Detection System, Attacks, Evolutionary Algorithms, Machine Learning Algorithms.

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) are infrastructure less networks with autonomous node are going to take part in communication. At any time the nodes in the MANET is free to enter or leave the network. All nodes in the MANET are self-configured and follow multi-hop routing nature. The nodes in the MANET have less battery power, small amount of computing capability. There is no central routing mechanism followed in MANETs. Due to the characteristics of MANET having limited bandwidth, low battery power, computational power, and security etc. security is a important aspect to be monitored. Due to the nature of MANETs, it is very evident that it leads to various attacks due to communication links between nodes, non-cooperation among nodes, and dynamic topology [1].

Intrusion detection seems to be any violating policies or abnormal activity take place in the network There will be a great danger in the modern digital era due to security breaches in the network due to various attacks. The prime motive of intrusion detection system is to deploy as a defensive parameter across any networks. It is able to detect any type of attacks that will able to compromise any nodes in network. Several types preventive mechanisms are deployed among networks to monitor any suspicious activity found in the network. Intrusion detection system can be classified in to signature based , specification based or anomaly detection[2]. Hybrid IDS combines both the feature of anomaly and signature based intrusion detection techniques. These techniques are useful in intrusion detection systems since an intrusion activity is different from the normal activity of the system.

Paper organization: We have a brief introduction about MANETs and Intrusion detection system. Section 2 describes security challenges related to Mobile Adhoc-Networks. Section 3 discusses the papers related to various types of intrusion detection system. Section 4 discuss existing design methodologies. Section 5 discusses the future work and conclusion work in design of intrusion detection system.

II. SECURITY CHALLENGES

Intrusion can be caused by unwanted users in the network attempt to gather additional requirements which are not actually authorized for them to use. Intrusion can be able to affect confidenality, integrity ,availability or to bypass the network structure. Due to the nature of mobile adhoc –network characteristics several nodes can be breached in the network due to several attacks attempt to invade the node in the network.

The preventive mechanism is broadly classified into the following types (i) Anaomaly Based (ii) Signature-based (iii) Hybrid. The anomaly based intrusion detection system is bale to detect attacks based on the abnormal activity of the node while signature based matches any type of attack based on their pre-stored attack charaterstics.Hybrid intrusion detection system is the combination of both anomaly and signature based. The following figure shows the typical arrangement of Intrusion detection system architecture where agents are deployed across the nodes for detetcion of any abnormal activity in the network.

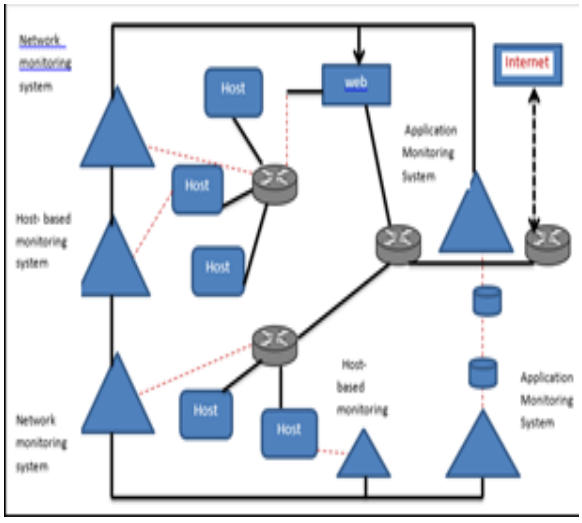

Fig 1: Architecture of Intrusion Detection System Architecture

Revised Manuscript Received on November 25, 2019.

***** Correspondence Author

Dilipkumar S*, Department of Computer Science & Engineering, BHARATHIDASAN UNIVERSITY, Trichy India. Email: sdilipkumar85@gmail.com

Dr.M.Durairaj, Dept. of CSE, BHARATHIDASAN UNIVERSITY, Trichy India. Email: durairaj.*bdu@gmail.com*

III. RELATED WORKS

The existing intrusion detection techniques are designed with traditional algorithms that will suffer from High false positive ratio, less detection rate and failed to detect multi stage attacks. The various techniques used in design of Intrusion detection system are discussed below. However, fuzzy rules are mainly based on expert knowledge from learning engines that are lack of adaptation [4]. The various techniques used in the intrusion detection system are discussed below,

S.No	Author	Attack Type	Technology Layout	Disadvantages
1	R J Cai et.al[1]	Collaborative	Self Checking Scheme(SCS) & ESCS(Enhanced SCS)	High end-end delay and overhead.
2	J.S.Park [2]	Collaborative	probabilistic analysis	Threshold level fixation is not a constant one. Leads to increase in False positive Ratio.
3	A.M.fahad et.al[4]	Collaborative	Harmony Search Algorithm(HAS)	Hello Message creates additional overhead.
4	C.W.Tsai [7]	Collaborative	IPSO classifiers	False Positive Rate increases
5	J. S. Park, D. H. Choi[8]	Collaborative	probabilistic analysis	False Positive Rate increases
6	P. Sharma, N. Sharma, and R. Singh[4]	Single	Secure IDS	parameters not clearly defined
7	P.M.Mafraa,,J.S.Fragaa,A.O.Santin c[5]	Collaborative	Distributed Algorithms	Assumes Next Neighbor is malicious free. Threshold level is also fixed depending on network condition.
8	Ning Weng Luke Vespa Benfano Soewito[6]	Single	Memory Base IDS-Adaptive method	System is complex and it is time consuming method.
9	Tie Wang, Gannan Wang, Yizhou Liu, Shuwen Zhou[7]	Single	Fuzzy based technique	Limits to specific type of attacks
10	Debjit Das, Koushik Majumder and Anurag Dasgupta[8]	Single	LTCF	Cost calculation on Route is difficult
11	Vivek K. Kshirsagar, Sonali M. Tidke & Swati Vishnu[9]	Single	Hybrid Technique	Discussed only Theoretical approach not any techniques to detect attacks
12	Sergio Pastrana, Aikaterini Mitrokotsa , Agustin Orfila , Pedro Peris-Lopez[10]	Collaborative	SVM classifier	False positive Rate increases
13	ShahaboddinShamshirband , NorBadrulAnuar , MissLaihaMatKiah , AhmedPatel[11]	Collaborative	collaborative-based wireless IDPS	Detection engine has to be modified
14	Sevil Sen , John A. Clark[12]	Collaborative	Evolutionary computation	Constrained resources performance decreases
15	Soumyadev Maity, R.C. Hansdah[13]	Single	certificate-less on-demand public key management	Verification of node delay increases due to some predefined rules
16	Sergio Pastrana , Juan E.[14]	Single	IDN model	Cost tradeoff is high

IV. EXISTING SYSTEM

The traditional system based design is not effective to detect any type of malicious activity when the attacker type is inside. All methods are focusing on the detection rate measures and attack prevention mechanisms while they fail to address false positive ratio, how they are able to address zero day attacks and future attacks also.

Current issues in intrusion detetcion system

1. Feature Extraction algorithms based on dataset are not efficient to detect attacks in effective manner.
2. Training of dataset using traditional algorithms is a time consuming process and it leads to increase in false positive ratio.
3. Overall intrusion detection performance like TP.FP.ROC characteristics will lead to significant decrease.

V. FUTURE WORK AND CONCLUSION

The intrusion detection system should be designed in such a way that is capable of detecting attacks based on a self-learning mechanism using evolutionary algorithms that having less false positive ratio and fast detection rate.
Intrusion design techniques have to be specifically designed for Tactical MANET scenario's where these networks have unique characteristics features that lead to capable of handling zero day attacks

REFRENCES

1. R. J. Cai, X. J. Li, and P. H. J. Chong(2016), "A novel self-checking ad hoc routing scheme against active black hole attacks," Security and Communication Networks, vol. 9 no. 10, pp. 943-957.
2. J. S. Park, D. H. Choi, Y. B. Jeon, Y. Nam, M. Hong, and D. S. Park (2017), "Network anomaly detection based on probabilistic analysis," Soft Computing, 2017. https://doi.org/10.1007/s00500-017-2679-3\
3. C. W. Tsai(2013), "Incremental particle swarm optimisation for intrusion detection," IET Networks, vol.2, no. 3, pp. 124-130.
4. R. Sharma, N. Sharma, and R. Singh(2012) "A secure intrusion detection system against DDOS attack in wireless mobile ad-hoc network," International Journal of Computer Applications, vol. 41, no. 21, pp. 16-21.
5. P.M.Mafraa, J.S.Fragaa, A.O.Santinc(2013)" Algorithms for a distributed IDS in MANETs", Journal of Computer and system Science".
6. Ning Weng Luke Vespa , Benfano Soewito(2011) ," Deep packet pre-filtering and finite state encoding for adaptive intrusion detection system",vol.55, pp. 1648-1661.
7. Tie Wang, Gannan Wang, Yizhou Liu, Shuwen Zhou(2011)" Fuzzy Reliability Design Based on Gamma and Normal Distribution", Second International Symposium on Intelligent Information Technology Application.
8. Debjit Dasa, Koushik Majumdera, Anurag Dasguptab(2015)" Selfish Node Detection and Low Cost Data Transmission in MANET using Game Theory,vol no.54, pp.no.92-101.
9. Vivek K. Kshirsagar, Sonali M. Tidke & Swati Vishnu(2014)" Intrusion Detection System using Genetic Algorithm and Data Mining: An Overview", International Journal of Computer Science and Informatics ISSN (PRINT): 2231 –5292, Vol-1, Iss-4.
10. Sergio Pastrana , Aikaterini Mitrokotsa , Agustin Orfila , Pedro Peris-Lopez(2012)" Evaluation of classification algorithms for intrusion detection in MANETs",Knowledge Based Sytems, Vol No. 36 pp.No. 217–225.
11. Shahaboddin Shamshirband NorBadrul Anuar, Miss Laiha Mat Kiah, Ahmed Patel(2013)" An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique", Engineering Applications of Artificial Intelligence, Vol No. 26 pp.No. 2105–2127.
12. Sevil Sen , John A. Clark(2011)" Evolutionary computation techniques for intrusion detection in mobile ad hoc networks, Computer Networks, Vol No. 53 pp.No. 3441–3457.
13. Soumyadev Maity, R.C. Hansdah(2011)" Self-organized public key management in MANETs with enhanced security and without certificate-chains", Computer Networks, Vol No. 65 pp.No. 183–211.
14. Sergio Pastrana ⇑, Juan E. Tapiador, Agustin Orfila, Pedro Peris-Lopez(2011) "DEFIDNET: A framework for optimal allocation of cyberdefenses in Intrusion Detection Networks", Computer Networks, Vol No. 80 pp.No. 66-88.

AUTHORS PROFILE

Dr.M.Durairaj, is working as Assistant Professor in Computer Science at School of Computer Science and Engineering, Bharathidasan University, Tiruchirappalli, Tamilnadu, India. He completed his Ph.D. in Computer Science as a full time research scholar at Bharathidasan University on April, 2011. He received master degree (M.C.A.) in 1997 and bachelor degree (B.Sc. in Computer Science) in 1993 from Bharathidasan University. He also worked as Research Associate at National Research Centre on Rapeseed-Mustard (Indian Council of Agricultural Research), Rajasthan, and as a Technical Officer (Computer Science) at National Institute of Animal Nutrition and Physiology (ICAR), Bangalore for 12 years. He has more than 98 research papers and 4 book chapters in his credit. He also completed three externally funded research projects. His areas of interest include Data Science, Cloud Computing and Artificial Intelligence.

S.DilipKumar is an Research Scholar in the Department of Computer Science & Engineering, Bharathidasan University, Trichy. He is currently working as a Assistant Professor in Dept. of CSE, Arasu Engineering, ,Kumbakonam.. His research area includes intrusion Detection system, Wireless networks, Network security.